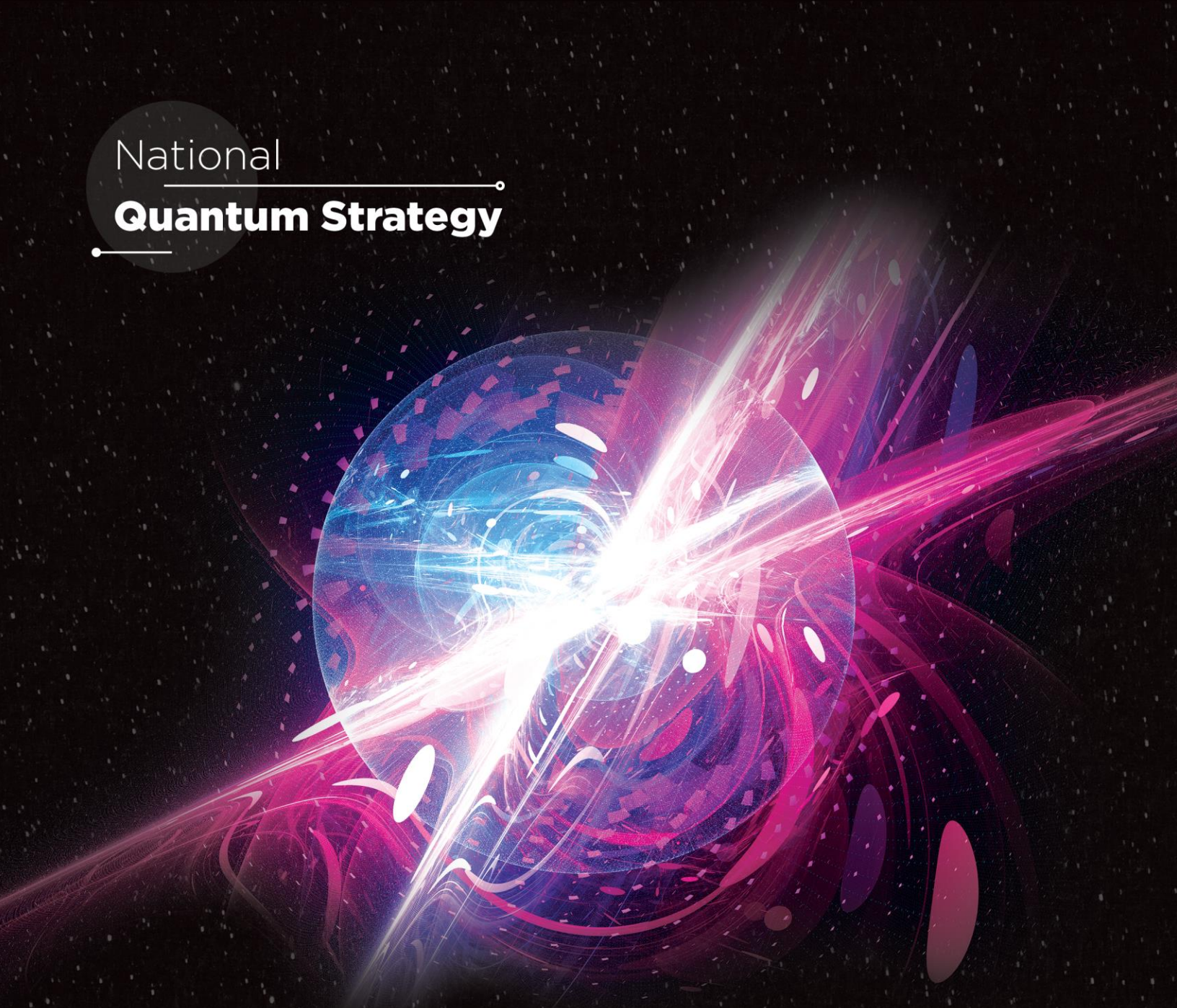
National
Quantum Strategy



National Quantum Strategy Roadmap

QUANTUM COMMUNICATION AND POST-QUANTUM CRYPTOGRAPHY

Government of Canada
Gouvernement du Canada

Canada

This publication is available online at https://ised-isde.canada.ca/site/national-quantum-strategy/en/national-quantum-strategy-roadmap-quantum-communication-and-post-quantum-cryptography

This roadmap is current as of February 17th, 2025 and may be updated from time to time. For the latest version of the roadmap, please visit the website.

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/publication-request or contact:

ISED Citizen Services Centre
Innovation, Science and Economic Development Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (international): 613-954-5031
TTY (for hearing impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: ised-isde@ISED-ISDE.gc.ca

Permission to Reproduce

Cat. No. Iu37-51/2-2024E-PDF
ISBN 978-0-660-74048-5

Aussi offert en français sous le titre *Feuille de route de la Stratégie quantique nationale : Communication quantique et cryptographie post-quantique*.

Table of contents

Introduction

Advances in quantum science have the potential to transform how people work and live. Investments over many decades have made Canada a global leader in quantum technologies and research, with a growing ecosystem of world-class centres of quantum expertise in universities and businesses across the country. As the rest of the world expands their own quantum strategies and initiatives, Canada must continue to invest wisely, innovate and commercialize to stay ahead while ensuring it is positioned as an integral contributor to the global supply chain.

To strengthen Canada's quantum ecosystem, the Government of Canada launched the National Quantum Strategy (NQS) in January 2023, and allocated $360 million in dedicated funding, in addition to leveraging a number of broad-based, large-scale programs. The NQS aims to: amplify Canada's strength in quantum research; grow quantum technologies, companies and talent; and solidify Canada's global leadership in quantum science and its commercialization. The NQS sets out three key missions on: quantum computing and software; communication and post-quantum cryptography; and sensors. To pursue these missions, NQS activities are supporting the three pillars of research, talent and commercialization. Success requires collective effort by many actors, including governments (federal, provincial, territorial and Indigenous governments and organizations), academia and industry, as well as non-profits such as incubators, accelerators and industry associations.

Road-mapping exercises engaged stakeholders to help identify challenges, gaps and opportunities, milestones and actions required to achieve success in each of the NQS missions. Provinces actively involved in the development of quantum hubs were engaged, and their input has been incorporated. However, other provinces and territories may also be undertaking actions to support quantum science and technology. Informed by these roadmaps, the Government is working with partners to advance the missions, and may explore additional investments.

This roadmap charts a course forward for the quantum communication and post-quantum cryptography mission. It will be updated periodically to reflect advances in quantum technologies that could drastically change timelines or lead to new applications.

Overview of quantum communication and post-quantum cryptography

This roadmap has two distinct, but related elements: developing a national secure quantum communication network and a post-quantum cryptography initiative. The timeframe differs with post-quantum cryptography (based on classical technologies) advancing in the short and medium term while a quantum communication network (based on quantum technologies) will take longer. The immediacy of

this mission is driven by technological advances that may lead to quantum computers that are capable of breaking many cryptography systems, including public key infrastructure (PKI), thereby threatening the security and privacy of digital systems and data. Both the Rivest-Shamir-Adleman (RSA) and the Elliptic-Curve Cryptography (ECC) algorithms will be vulnerable to cryptographically-relevant quantum computers (CRQC) implementing Shor's algorithm. CRQCs have not yet been created and estimates vary on their arrival. However, information requiring long term protection needs to be secured now prior to the deployment of a CRQC, as today's encrypted information can be accessed, copied, stored and compromised in the future when CRQCs are available. This threat is also known as: 'harvest now, decrypt later'.

To address these challenges, post-quantum cryptography (PQC), also known as quantum-safe or quantum-resistant cryptography, is being developed. PQC enables cryptographic systems to be resistant to attacks from quantum and classical computers, and has advanced to standardization.[1] Migration to PQC can start in the short-term with adaptations to existing cryptographic systems and protocols.

The security of PQC key establishment algorithms relies on the intractability of certain well-studied mathematical problems against algorithms on both classical and quantum computers. By contrast, quantum communication allows key establishment protocols, such as quantum key distribution (QKD), whose security does not rely on intractable mathematical problems but rather on the fundamental principles of quantum mechanics. Although QKD could provide higher confidence that transmitted data remains secure, significant technical challenges remain before there can be widespread deployment.

A quantum communication network can also facilitate distributed and blind quantum computing[2] and long-baseline sensing, supporting the other NQS missions. This could increase quantum computing processing power and effectiveness of quantum sensors.

Ultimately, a national quantum communication network based on QKD together with PQC could enhance the security of information for critical infrastructure. Combining multiple solutions allows a flexible network, including land and satellite-based infrastructure, to store and transmit sensitive information and ensure interoperability with international partners.

There is an immense global commercial market tied to transmitting and securing data and increasing the interconnectedness of devices. An NRC-commissioned study estimated the market for quantum encryption alone expected to reach US$4.7B in 2033, growing at a compounded annual growth rate of 27%.[3] Major end-users include IT and telecommunications, finance, defence, healthcare and natural resources/energy sectors. Developing and scaling-up Canadian innovations will help increase returns for Canada.

[1] Cyber Centre celebrates new NIST post-quantum standards - Canadian Centre for Cyber Security
[2] Blind quantum computing connects separate quantum computing entities in a secure way which allows users to perform remote computations on a remote server without revealing their data or algorithms to the server.
[3] Doyletech Corporation, *Quantum Canada: Social-Economic Impact Assessment 2023 Update*. 2024.

Quantum communication and post-quantum cryptography mission

Ensure the privacy and cyber-security of Canadians in a quantum-enabled world through a national secure quantum communication network and a post-quantum cryptography initiative.

To achieve this mission, work will advance on PQC, QKD and quantum communication technologies to ensure that existing and future communications and data systems are protected in addition to supporting distributed quantum computing and sensing.

To address the urgent threat of 'harvest now, decrypt later' and vulnerability against early quantum-enabled adversaries, immediate actions are required on implementing a **post-quantum cryptography initiative.** The following priorities have been identified:

- raising awareness of the threat from CRQCs and mitigation actions to be taken
- supporting the development, testing and standardization of PQC schemes and adoption in cybersecurity protocols
- migrating existing cryptographic systems to PQC

Over a longer time horizon, developing a **national secure quantum communication network** will advance quantum computing and sensing and enhance the security of communications. The following priorities have been identified:

- addressing scientific and technical barriers to quantum networking
- building a national integrated quantum network test bed, with satellite and ground fibre-optic based links and associated components
- identifying use cases and proofs-of-value for receptor industries and supporting engagement with vendors and end-users
- ensuring interoperability through international standardization and partnerships
- reducing supply chain gaps and developing domestic manufacturing capacity

To **support the quantum communication and PQC ecosystems** in general, the following priorities need to be advanced:

- strengthening the talent pipeline
- promoting the Canadian quantum communication and PQC sector domestically and internationally
- addressing barriers to growth for Canadian quantum communication and PQC companies
- identifying societal impacts and developing an ethics framework
- protecting intellectual property (IP) and improving the security posture of Canadian researchers and innovators

Programming supporting the quantum communication and PQC mission

Work on this mission has already begun. The Government of Canada, led by the Communications Security Establishment (CSE), has undertaken activities to ensure that its highly sensitive data holdings are protected against the quantum threat. These activities are coordinated with international allies to maintain interoperability. The identification of Government systems and data that are less sensitive but still potentially at risk is an ongoing effort and plans are being made to secure them using PQC.

CSE is also providing technical guidance to organizations and the Canadian public on the transition to PQC in addition to participating in the United States' National Institute for Standards and Technology (NIST) Post-Quantum Cryptography Standardization Process and supporting the adoption of PQC in other standards development organizations. For example, CSE, Shared Services Canada (SSC) and Innovation, Science and Economic Development Canada (ISED) are members of the Quantum-Readiness Working Group of the Canadian Forum for Digital Infrastructure Resilience. CSE provides technical advice on the Working Group's Canadian National Quantum-Readiness: Best Practices and Guidelines produced in cooperation with members of Canada's financial sector. CSE, Treasury Board of Canada Secretariat and SSC are preparing and planning for the transition of Government systems. Public Safety Canada, ISED and CSE are working with critical infrastructure partners, including industry, provincial, territorial and municipal governments, to ensure Canada's critical infrastructure is protected from the threat posed by CRQC.

Many other programs and initiatives across the Government of Canada are already supporting the quantum communication and PQC mission:

- the Government of Canada initiated the Quantum Encryption and Science Satellite (QEYSSat) project with academic institutions and private partners, one of the first tests of satellite-based secure quantum communication demonstrations, expected to launch in 2025-26
- the National Research Council of Canada's (NRC) High Throughput and Secure Networks Challenge Program has been supporting collaborative R&D projects on quantum communication with industry, academia and other government departments since 2019
- in June 2022, Innovative Solutions Canada (ISC) launched a call to support pre-commercial quantum communication prototypes that can be tested in real-life settings and address federal government priorities
- the Natural Sciences and Engineering Research Council of Canada (NSERC) announced $51 million in awards to 75 recipients in quantum science and technology through the Alliance and Collaborative Research and Training Experience (CREATE) programs in April 2023
- Canada Economic Development for Quebec Regions in 2023 announced $3.6 million for Numana to set up telco-grade aerial and underground fibre optics quantum communication testbeds in Montréal, Québec and Sherbrooke. The testbed will also have a link to the QEYSSat project via the Canadian Space Agency ground station in Saint-Hubert.

Furthermore, the Department of National Defence/Canadian Armed Forces released its Quantum Science and Technology Strategy Implementation Plan, Quantum 2030, in 2023. It identifies four quantum technologies with defence applications and lays out a seven-year plan to develop prototypes, including quantum communications (quantum networking), to be tested in the field by 2030.

Fundamental research that aims to advance our understanding of the science underlying future breakthroughs is important for success and is supported through existing mechanisms such as NSERC Discovery Grants.

Applied research that aligns with the three NQS missions is funded through calls under NSERC Alliance and ISC. Business and non-profit support will continue through the Industrial Research Assistance Program (IRAP), Strategic Innovation Fund, Regional Development Agency programming, Global Innovation Clusters, Strategic Science Fund, Innovation for Defence Excellence and Security, Deep Tech Venture Fund, etc.

The Government is also taking action on cyber security more broadly. The 2018 National Cyber Security Strategy guides the Government of Canada's cyber security activities to safeguard Canadians' digital privacy, security and economy. Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* (*ARCS*), introduced in 2022, aims to protect Canadians and bolster cyber security across the financial, telecommunications, energy, and transportation sectors.

1. Post-quantum cryptography

Post-quantum cryptography (PQC) refers to cryptographic algorithms that are resistant to attacks by a CRQC using existing algorithms for data-in-motion and data-at-rest. Existing public key cryptography can be migrated to PQC to maintain interoperability with existing communication protocols, software, and networks.

Given the threat of 'harvest now, decrypt later', raising awareness of the threat to existing encryption systems, and of the necessary mitigations is key. While work continues on the testing and standardization of PQC and its adoption within cybersecurity protocols, organizations must take steps to be cryptographically agile (the ability to quickly transition cryptography in a deployed system) and be up to date with the latest standards, including adopting PQC. This includes cataloguing existing cryptography usage, prioritizing sensitive data with long lifespan for PQC migration and identifying migration pathways.

Once PQC algorithms are standardized there will be a need to update product certification programs to test PQC, such as the Cryptographic Module Validation Program (CMVP) jointly managed by CSE and NIST, as integration into popular cryptographic libraries and vendor products will be essential. Certified cryptographic products containing validated PQC could be on the market by 2026.

At the same time, R&D will continue on other cryptographic approaches for situations not covered by generic key-establishment and digital-signature PQC schemes. Testing, standardization, certification and adoption should also follow. CSE, as Canada's technical authority for cybersecurity and information assurance, will continue to provide expert advice and support on cyber security.

Current status

Canada

Canada is a pioneer in the development of PQC solutions. Canadian researchers are consistently featured at international conferences and founded the Open Quantum Safe project. They also play a significant role in the NIST PQC Standardization Process, having co-authored two of the four schemes already selected for standardization. Furthermore, the Government of Canada, through the CSE, has contributed to the NIST standardization effort. Canada is also home to some of the world's leading PQC companies.

NIST has published three PQC standards in August 2024, with more to follow. This standardization is expected to begin widespread transition to PQC. The Government of Canada is also participating in international standardization processes, critical infrastructure partnerships and industry engagements with stakeholders to encourage the adoption of NIST-recommended PQC in standards, industry specifications and commercial products.

International

While there is no common global standard, many countries are awaiting standardization by NIST. For example, the European Telecommunications Standards Institute (ETSI) Quantum-Safe Cryptography working group has publications on migration to PQC (ETSI TR 103 619) as well as technical reports on NIST candidates (ETSI TR 103 823, among others). Non-algorithmic work undertaken by this working group includes the standardisation of PQC architectures, implementation techniques, performance evaluation methods and migration methodologies to post-quantum systems. Many other standards bodies are also working on PQC.[4]

In addition, existing and forthcoming standards from both the IETF and ETSI are enabling the use of pre-shared keys in network protocols, to facilitate quantum-secure communications.

Key challenges

Although PQC has largely moved beyond the academic research stage, numerous challenges remain on both the technical and organizational aspects of migration. Transitioning cryptographic algorithms has historically been a slow process. Previous standardized cryptographic primitives that have been

[4] Standards bodies such as International Standards Organization (ISO) Joint Technical Committee 1 (JTC 1) Sub-Committee 27 (SC27), International Telecommunications Union Telecom Sector Study Group 17 (ITU-T SG17), Institute of Electrical and Electronic Engineers (IEEE) Standards Organization and American National Standards Institute (ANSI) Group X9 are active on PQC. Specifications for the adoption of PQC in network protocols are being developed at the Internet Engineering Task Force (IETF).

deprecated are still in use.[5] The transition to PQC will be significantly broader than past cryptography transitions, take longer and require more effort.

Lack of awareness and organizational challenges

Many organizations are not aware of the seriousness, urgency and relevance of the threat posed by a CRQC. Executives, managers and technical teams must become cognizant of this risk, so that they can make strategic decisions and allocate appropriate resources to the transition to PQC. Training within firms, along with raising awareness of the management of innovation required to adopt disruptive technology is important. Guidelines will be developed and regulations put in place, when and where appropriate, to ensure that critical data is protected.

Standardization

Vetted standards for PQC are critical to ensuring the trust and security of cryptographic solutions. Furthermore, it will be important that the NIST PQC standards are globally accepted, as competing standards may lead to fragmentation. Nonetheless, even standardized algorithms may later be proven vulnerable. Continually testing PQC algorithms and developing additional ones will be necessary.

Global migration

Given the interconnectedness of data systems, migration to PQC by a single organization, sector, region or country will not be sufficient. Migration must be widespread to avoid vulnerabilities in weak links within the network. Global migration to PQC is critical as Canadian data transiting international networks could be collected and stored by our adversaries.

Technical challenges to implementation

Some of the proposed PQC solutions are expected to have a significant increase in the sizes of stored and transmitted cryptographic objects and/or computation time, creating a negative performance impact especially in resource-limited environments.

Cryptographical protocols beyond key-establishment and digital signature

The NIST standardization process has identified key-establishment and digital signature algorithms. These are the most important primitives, providing the essential properties of confidentiality, integrity and authentication. However, there are cryptographic protocols in use which cannot leverage the NIST algorithms and where it can be a significant research challenge to make them quantum-safe. Examples include password-authenticated key exchange protocols, ratchet-based instant-messaging systems, anonymous attestation, unlinkable digital credentials and the cryptography employed by some distributed ledger systems.

Vendor support for PQC

Cryptographic agility might be advanced by working with software and hardware vendors, even if they are using open-source solutions. Vendors need long lead times to develop cryptographic capabilities and have them certified. To ensure that cryptographic solutions and products will be available during the

[5] Examples of deprecated cryptographic primitives still in use include hashing algorithms MD5 and SHA1, symmetric encryption schemes DES and 3DES, and lower parameter sets of public key algorithms like RSA 1024.

transition to PQC, the Government can communicate the need for these products in advance. This will stimulate demand from end-users and incentivize vendors to develop PQC products.

Action plan

The objective in the long-term (by the 2030s) is to **complete Canada's transition to post-quantum cryptography.** The action plans below indicate short (0-3 years) and medium term (3-7 years) actions to achieve this objective.

Raising awareness of the quantum threat and mitigation actions to be taken

Raise awareness of the quantum threat and the need for action through training programs

Action item	Timeline	Lead
A1a. Develop: • quantum-safe curriculum for universities, colleges, polytechnics and private training centres across Canada • quantum-safe certifications for quantum-safe programs and their graduates • training modules related to quantum threats for trainees, executives and compliance teams	Short term	Academia
A1b. Implement quantum-safe curriculum, certifications for training programs, and training modules	Medium term	Academia
A2. Industry to: • support job integrated learning and on-the-job training • establish education programs to support industry awareness of post-quantum cryptography	Short and medium term	Industry/Non-Profit

Encourage awareness among Canadian industry to achieve quantum resiliency

Action item	Timeline	Lead
A3. Communicate quantum resiliency priorities of the Government of Canada to industry and work with key sectors to raise awareness of quantum resiliency and develop cryptographic agility	Short and medium term	Government of Canada, Industry/ Non-Profit

Provincial actions (as submitted)

Action item	Timeline	Lead
A4. Leverage the GoA Cybersecurity division's CyberAlberta program and Community of Interest to raise awareness of the quantum threat which poses significant risks to society and business by disrupting encryption algorithms and protocols used in Alberta's core industries, leading to data breaches and damage to infrastructure	Short and medium term	Government of Alberta

A5. Working with quantum and cybersecurity experts, develop educational programs and qualifications to build B.C.'s skilled post-quantum security and industry workforce to assist businesses and organizations to adopt quantum solutions and prepare for post-quantum impacts	Short and medium term	Government of British Columbia
A6. Work with B.C. companies, educational institutions, and industry associations to raise awareness of PQC	Short and medium term	Government of British Columbia
A7. Work with subject matter experts from institutions to raise awareness	Short and medium term	Government of Ontario
A8. Québec's Ministry of cybersecurity and digital affairs coordinates with other provincial governmental actors and key players in the ecosystem to raise awareness of the quantum threat in all sectors	Short and medium term	Government of Québec

Supporting the development, testing and standardization of PQC schemes and adoption in cybersecurity protocols

Test and standardize PQC key establishment and digital signature schemes

Action item	Timeline	Lead
A9. Continue security analysis and testing of PQC schemes	Short and medium term	Academia
A10. Continue developing algorithms, libraries, and integration into protocols and applications, including for open-source software	Short and medium term	Academia, Industry/ Non-Profit
A11. Participate in international standard development processes	Short and medium term	All
A12a. Develop and accredit conformance testing of PQC through cryptographic certification programs	Short term	Government of Canada, Industry/ Non-Profit
A12b. Continue to update certification programs to support new PQC standards	Medium term	Government of Canada, Industry/ Non-Profit
A13. Periodically audit systems to confirm compliance with current PQC standards	Medium term	Industry/ Non-Profit

Develop, test, and standardize additional cryptographic approaches

Action item	Timeline	Lead
A14. Undertake R&D and testing of additional post-quantum cryptographic approaches	Short and medium term	All

A15. Participate in standardization of additional post-quantum cryptographic approaches	Short and medium term	All

Develop manufacturing capacity for PQC hardware

Action item	Timeline	Lead
A16. Establish a fabrication ecosystem around the anchor companies producing PQC hardware in Canada	Short and medium term	Industry/ Non-Profit

Provincial actions (as submitted)

Action item	Timeline	Lead
A17. Undertake R&D and testing of additional cryptographic approaches that are harder to break to safeguard against cyber intrusion	Short and medium term	Government of Alberta
A18. Work with B.C. businesses, government organizations and public utilities to implement the recommendations of Canada's National Working Group on Post-Quantum Readiness	Short and medium term	Government of British Columbia
A19. The development and testing of PQC schemes are part of Québec's quantum communication initiative (see Secure national quantum communication network action plan, B21, below)	Short and medium term	Government of Québec

Migrating existing cryptographic systems to PQC

Transition to PQC for non-Government of Canada systems

Action item	Timeline	Lead
A20. Plan for PQC migration including creating an inventory of current cryptography risk assessments for information holdings and budgeting for migration	Short term	Industry
A21a. Begin PQC migration once standards are available	Short term	Industry
A21b. Upgrade PKI and transition to PQC	Medium term	Industry
A22. Develop guidelines and regulations on post-quantum security for key at-risk sectors	Medium term	Government of Canada

Ensure that Government of Canada systems are protected against the quantum threat

Action item	Timeline	Lead
A23. Identify and prioritize systems of importance to Canada for cryptographic transition	Short term	Government of Canada
A24. Identify and catalogue cryptography usage in existing information systems	Short and medium term	Government of Canada
A25. Communicate future PQC related procurement needs to the vendor community so that they can begin development of products and incorporate quantum-safe requirements in procurement	Short and medium term	Government of Canada

A26. Transition Government of Canada systems to PQC	Medium term	Government of Canada
A27. Periodically audit systems to confirm compliance with current PQC standards	Medium term	Government of Canada

Provincial actions (as submitted)

Action item	Timeline	Lead
A28. CyberAlberta to lead and facilitate efforts for quantum threat readiness across Alberta's public and private sector by leveraging the CyberAlberta Community of Interest	Short and medium term	Government of Alberta
A29. Launch and implement Alberta's Quantum Tech Framework	Short and medium term	Government of Alberta
A30. Work with B.C. businesses, government organizations and public utilities to implement the recommendations of Canada's National Working Group on Post-Quantum Readiness	Short and medium term	Government of British Columbia

2. Secure national quantum communication network

A quantum communication network enables quantum information exchange through quantum communication channels, assisted by classical channels. Such a network enables quantum cryptography, of which the most well-established approach is quantum key distribution (QKD), a secure communication method that involves the generation and encoding of encryption keys in a quantum state using qubits. In QKD, any eavesdropping activity or outside interference will be detected by the communicating users. In this way, QKD is theoretically unhackable and secure against computing and algorithm advances.

Quantum communication networks can also increase the performance of, or enable new functionality for, quantum computers and quantum sensors.

Significant research and development effort is required to achieve this mission. Several areas of focus have been identified to develop a secure national quantum communication network:

Integrated national testbed, collaboration and coordination

A national testbed that integrates both ground and satellite-based quantum links will improve collaboration and coordination. This could incorporate existing infrastructure and projects, such as QEYSSat, provincial and regional quantum communication network infrastructure.

Sharing infrastructure with academia, industry, not-for-profit and government will increase the pace of development. Building a national-level testbed will also help demonstrate that quantum communication is a priority for Canada, and will allow us to attract, develop and retain talent from Canada and abroad.

Use cases and market development

Identifying use cases and engaging with end-users will help develop a domestic market, leading to further investments. In addition, engaging end-users will direct R&D to commercially relevant areas, improving possibility for commercialization. Multi-disciplinary research on societal and technological impacts can also enable future applications.

Beyond QKD, a quantum network has the potential to enable distributed quantum computing and blind quantum computing, greatly scaling processing power and enabling private encryption and authentication. It may also enable dense coding of information and oblivious transfer of information.[6]

Furthermore, the network could allow for distributed quantum sensing, with applications such as quantum enhanced telescopes or improved clock synchronisation and global positioning systems (GPS). This network can further improve quantum metrology with the ultimate scope of enhancing measurement precision.

Current status

Canada

Canada is home to pre-eminent researchers and companies developing QKD to secure valuable data and other advances in quantum networking. Dr. Gilles Brassard was one of the co-inventors of the first quantum cryptography protocol[7] and with Dr. Claude Crépeau were among the co-authors of the first paper on quantum teleportation[8]. Canadian researchers have invented additional QKD protocols including measurement-device-independent (MDI) QKD. Canada is also a leader in the security analysis of practical QKD systems including treatment of implementation security (side-channels). They have also invented or played key roles in the advance of multi-party computing and quantum memories.

Although ground-based QKD devices are commercially available today, their capacity is limited. Existing systems use fibre optic cables to transmit photons on land but the signal becomes unreliable over large distances mainly due to losses in fibre, which deteriorate the quantum signal. Advancing quantum repeaters and memories are key as they can extend the transmission range and are likely to form the backbone of large-scale quantum communication networks. In addition, transcontinental, satellite links as well as integration of post quantum cryptography and existing forms of communication technology will be necessary.

Canadian researchers are at the leading edge in the development of quantum communication research and satellite networks. QEYSSat, funded by the Canadian Space Agency (CSA), is expected to launch in 2025-26 and will demonstrate QKD from space.

[6] Oblivious transfer is a two-party protocol between a sender and a receiver, where the sender transfers some information to the receiver, but the sender is oblivious/does not know what information the receiver actually obtains.
[7] Bennett, Charles H. and Brassard, Gilles, *Theoretical Computer Science*, Vol. 560 (Part 1), 2014, pp. 7-11; Lo, Curty, and Qi, *Phys. Rev. Lett*. 108, 130503 (2012); Xu et al. Mod. *Phys.* 92, 025002 (2020).
[8] Bennett, Charles H.; Brassard, Gilles; Crépeau, Claude; Jozsa, Richard; Peres, Asher; Wootters, William K. (29 March 1993). "Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels". *Physical Review Letters*. 70 (13): 1895–1899.

Quantum EncrYption and Science Satellite (QEYSSat)

QEYSSat is a low-earth orbit (LEO) satellite with a quantum receiver capable of exchanging quantum-encoded information through photons with a quantum ground station via a free-space link. Individual photons will be sent through a laser link from a ground station to a microsatellite, which will use the QKD protocol to establish a key. A key shared by two ground stations can be created by treating the satellite as a secure node. The satellite will also include a quantum transmitter. This trial will allow scientists to study how QKD behaves in space, and lay the groundwork for a global quantum communication network.

The QEYSSat User Investigation Team (QUINT) consortium brings together 19 researchers and government and industry partners for research on Canadian quantum communication satellite missions, including QEYSSat. This project aims to design and demonstrate the building blocks and concepts of a future Canada-wide quantum internet and will begin by conducing research related to QEYSSat, such as studies on uplink and downlink quantum links. The project will also research future implementations of quantum communication networks with satellites.

In 2022, the Institute for Quantum Computing led a study funded by the NRC and Defence Research and Development Canada that proposed a next-generation satellite mission, QEYSSat 2.0, for long range quantum teleportation as a crucial next step to a Canadian quantum internet.

Canadian researchers are also pioneers in ground-based quantum communication. A 2016 project led by University of Calgary researchers successfully demonstrated teleportation of a photon over a distance of six kilometres using the City of Calgary's fibre optic infrastructure, setting a then-record for distance of transferring a quantum state by teleportation. Researchers at the University of Toronto were the first in the world to implement the decoy state protocol and to successfully hack commercial QKD systems. In 2022, they became the first in the world to implement a novel twin-field QKD network.

ARAQNE (Alliance for Research and Applications of Quantum Network Entanglement) project

ARAQNE advances the platforms for QKD-secure communication as well as alternative entanglement-based cryptography solutions that harness quantum mechanics' advantages for the full range of quantum communication (beyond key sharing). In particular, ARAQNE will include activities focussed on enabling true long-distance terrestrial communications through quantum repeaters.

As limitations in qubit number are present in all current quantum processing units (QPUs), distributing operations is a promising path to larger-scale calculations, laying the groundwork for larger-scale computations that will be possible as QPUs advance. Through developing a broad suite of quantum networking tools and protocols, ARAQNE will lay the groundwork for long-distance distributed computing, including blind and homomorphic quantum computing.[9]

In October 2022, Numana launched a quantum communication network by optical fibre in Sherbrooke in partnership with the Government of Quebec, Bell Canada, and DistriQ. The testbed provides access to telco dark fibre optics networks thus allowing the connection of quantum related devices (e.g., computers, simulators, sensors) by telecom links. The testbed is also configured for testing adoption

[9] Homomorphic-encrypted quantum encryption allows computations on encrypted data without decrypting them.

related cases. Presently, QKD equipment, including key management systems, are available. Additional testbeds are expected to launch in Montreal in June 2024 with TELUS as the telco partner and Quebec City by end of 2024, with the goal of being linked into a provincial, and eventually national, network.

In addition, Canada has several national and international partnerships to advance quantum communication. New federally supported consortia have been established such as the Alliance for Research and Application of Quantum Network Entanglement (ARAQNE), Hybrid Quantum Interfaces (HQI), Québec Ontario consortium on quantum protocols (QUORUM), NRC Quantum Research and Development Initiative Quantum Application, Networks and Devices (QuAND), and Quantum and Artificial Intelligence Light Infrastructure for Tomorrow Sustainable Systems (QUALITY). In 2023, HyperSpace, a collaboration between researchers in Canada and Europe on studying high Earth orbit satellite QKD transatlantic entanglement, was announced. The University of Waterloo is also working with the United Kingdom on BaSQuaNa (Building a Standardized Quantum-Safe Networking Architecture) to develop the first open-source transatlantic QKD network.

The technological and scientific expertise already exists in Canada to support a national quantum communication network. Canadian experts have made significant progress in building blocks of a quantum network, including experimental demonstration of quantum memories, microwave-to-optical photon conversion, quantum teleportation, quantum cryptography, free-space QKD, fibre-based QKD protocols through ultrafast discrete time-entangled (time bins) photonic qudits, theoretical studies on quantum transduction, quantum repeaters, satellite-based quantum communication, quantum random number generators and global quantum networks. In addition, Canadian firms are at the forefront of commercializing quantum communication R&D, offering cutting-edge solutions that are already available on the market.

HyperSpace (Hyper-entanglement in Space) project

HyperSpace aims to extend the untapped potential of high-dimensional entangled photons to achieve long-distance free-space communications and entanglement distribution between Canada and Europe. Photons that are entangled in d-dimensions (qudits) can store more quantum information than qubits (2-D). Using qudits can increase the overall channel capacity, as well as improve resilience with respect to noise, losses, and eavesdropping in QKD. HyperSpace encompasses research and innovation along the complete chain of photonic quantum communications, from noise-resilient state encoding, to fully fibre and photonic integrated quantum light sources, to free-space compatible state analyzers. HyperSpace offers a unique opportunity to create a Canadian/European space link thanks to the shared expertise of the Canadian and European partners.

International

Quantum communication networks have been planned or already set-up around the world, ranging in scale from city-wide networks to intercontinental systems. In 2020, the US announced the ‘Blueprint for the Quantum Internet’, which lays out a plan to build the first large-scale quantum networks in the US. Similar efforts are underway around the globe, such as the Quantum Internet Alliance and the European Quantum Communication Infrastructure (EuroQCI) initiative in Europe.

Advances in quantum communication links continue at a rapid pace. Researchers in Switzerland and China have demonstrated ground fibre optic QKD links beyond 1,000 km. Numerous city-wide quantum-safe networks have been developed or are being established across the world. For example, a quantum

network in Hefei, China, supports multiple users simultaneously, using three devices, a central server and quantum memories. Additionally, three new protocols for generating verifiable quantum entanglement between two nodes in a network have been developed independently by teams in China, Europe and the US. The research, which allows distant quantum memories to exchange quantum information, may constitute a step towards a quantum version of the Internet in which photons travelling down standard optical fibres are used to entangle spatially separated quantum computers.

The Chinese Academy of Sciences has launched Micius, the world's first major quantum communication LEO satellite. This satellite has demonstrated direct distribution of entangled photon pairs over 1,200 km, secure QKD over intercontinental distances between China and Austria, and ground-to-satellite quantum teleportation of independent single photon qubits over distances up to 1,400 km. More recently, a hybrid quantum communication network over 4,600 km was demonstrated using an existing trusted node link between Beijing and Shanghai, China with a satellite-to-ground free-space link.

Key challenges

Coordination

Given the complexity and challenges of developing a national secure quantum network, it will be essential to coordinate between different organizations and sectors, as well as across borders to develop new solutions, ensure compatibility and drive standardization.

Investments and markets

While the potential global market for quantum communication is immense, significant investments will be required to achieve this mission and secure a portion of this market. Many investors perceive quantum communication as too costly and this issue is compounded by small near-term demand, which is related to the lack of use-case development and marketing.

Technical challenges

Technical challenges in quantum communication broadly fall under three themes: developing new technologies; refining existing technologies and information-transfer protocols; and developing or upgrading network infrastructure while ensuring maximum interoperability with existing infrastructure.

There are three main hurdles that new technologies will need to be addressed:

1. quantum repeaters are needed to extend the reach of quantum networks
2. robust quantum memory devices that are compatible with communication networks will need to be created to preserve entanglement
3. quantum satellite links must be refined to expand the network coverage

Critical technologies needed to reach these goals include: single photon detectors; both non-deterministic and deterministic high generation rate quantum sources; quantum repeaters based on photonics; improved quantum memories; and quantum error correction. Other components such as Quantum Random Number Generators (QRNGs) with certifiable randomness and based on heralded single-photon sources rather than on attenuated lasers to avoid multiphoton attacks, could improve the security of cryptographic algorithms, potentially supporting PQC algorithms and QKD. Entangled qudits could also increase channel capacity and improve performance.

Existing technologies and protocols will need to be refined or incorporated within quantum communication networks. This includes quantum communication protocols; adaptive optics for wave-front correction; simulation of quantum networks to improve network design; and for near-term applications, integration with existing telecommunication infrastructure.

Security analysis and certification of devices and systems are also required. This includes integration of PQC and QKD devices and infrastructure, authentication of end-points, and the physical and digital protection of quantum communication infrastructure.

Integration into global supply chains and developing manufacturing capabilities

A practical long-range quantum communication network may require space-based components as well as ground-based links to address the long distances. In many cases these materials and components are not currently produced in Canada or not at sufficient levels to meet anticipated demand. Canadian capabilities must be developed either domestically or in partnership with allies who are able to contribute the components and expertise we lack.

Capturing more of the supply chain for development activities inside Canada can increase supply chain resiliency and security, generate economic growth, and foster innovation and collaboration. Discussions between the government and the quantum community can help determine the necessity and feasibility of a domestic footprint for quantum communication components. In cases where key components are only available internationally, establishing agreements to secure Canadian access may be necessary. Enhancing our comprehension of the global supply chain and determining Canada's role within it will be necessary.

Action plan

The objectives in the long-term (7+ years) are to:

- create a secure quantum communication network linking inter-city or telecom switching stations through fibre and satellite-based links, and achieving quantum teleportation across Canada
- achieve global quantum communication through fibre optic quantum repeaters and/or satellite-based links
- establish a fabrication ecosystem around the anchor companies producing key quantum communication components in Canada
- ensure that Canada is a world leader in the global trade of quantum communication products and services, and a contributor to international standards

The action plan indicates short (0-3 years) and medium term (3-7 years) actions to create a secure national quantum communication network.

Address scientific and technical barriers to quantum networking

Action item	Timeline	Lead
B1. Support basic and applied research, development and technology demonstrations.	Short and medium term	Government of Canada

B2a. Develop: • prototype quantum up/down-links • quantum cryptographic components • architecture for quantum-classical interaction	Short and medium term	Academia, Industry/Non-Profit
B2b. Develop: • quantum repeaters to extend the reach of quantum networks • quantum memories to preserve entanglement	Medium term	Academia, Industry/Non-Profit
B3. Refine and develop quantum communication and QKD protocols including security analysis for certification.	Short and medium term	Academia, Industry/Non-Profit

Create a national quantum network test bed

Action item	Timeline	Lead
B4a. Identify, support, launch and participate in a national integrated quantum network test bed, with satellite and ground fibre-optic based links, PQC integration and associated components to test/demonstrate secure data transmission and networking for quantum computing and sensing	Short and medium term	Government of Canada, Academia, Industry/Non-Profit
B4b. Establish a cross-sectoral working group to study and plan for the national quantum network test bed	Short term	Government of Canada, Academia, Industry/Non-Profit

Identify use cases and proofs-of-value for receptor industries and support engagement with vendors and end-users

Action item	Timeline	Lead
B5. Engage receptor industries and identify use-cases and proofs of value	Short and medium term	Industry/Non-Profit
B6. Assess investing in test pilot projects where end-users in key sectors can test applications	Short and medium term	Government of Canada
B7. Assess supporting industry adoption by offsetting research and development and implementation costs by sectors likely to adopt quantum communication applications	Short and medium term	Government of Canada
B8. Communicate future Government quantum communication procurement needs to vendors so that they can begin development of products	Medium term	Government of Canada
B9. Support proof-of-concept projects within Government on uses of quantum communication	Medium term	Government of Canada

Ensure interoperability through international standards development and partnerships

Action item	Timeline	Lead
B10. Identify and participate in international standards development activities	Short and medium term	All
B11. Develop certification abilities for quantum communication devices	Medium term	Government, Industry/Non-Profit
B12. Collaborate internationally to accelerate development of quantum communication and cryptography applications	Short and medium term	All

Reduce supply chain gaps and develop domestic manufacturing capacity

Action item	Timeline	Lead
B13a. Identify key supply chain gaps and priority areas to develop Canadian manufacturing capacity of quantum communication components. Identify how Canada should be integrated into the global supply chain	Short term	Industry/Non-Profit
B13b. Begin development of manufacturing capacity for quantum communication components	Medium term	Industry/Non-Profit
B14. Protect quantum communication supply chain and establish access to internationally-produced materials and technologies with international agreements or other mechanisms	Short and medium term	Government of Canada

Provincial actions (as submitted)

Action item	Timeline	Lead
B15. Collaborate with other provinces and industry to gain access to quantum technology infrastructure to support research in quantum communication and cryptography	Short and medium term	Government of Alberta
B16. Drive the development of transdisciplinary solutions that address global challenges through the application of quantum technologies	Short and medium term	Government of Alberta
B17. Accelerate industry-academic collaboration in quantum communication and cryptography	Medium term	Government of Alberta
B18. Support technology collaboration between Alberta companies and international companies in quantum communication and cryptography	Medium term	Government of Alberta
B19. Support the creation of a B.C. quantum networking and communications test bed to test and showcase quantum communications technologies, collaborating with national and provincial networks, as appropriate	Short and medium term	Government of British Columbia
B20. Collaborate with the industry on quantum communication and cryptography to share knowledge and resources and make efforts to develop a comprehensive framework	Short and medium term	Government of Ontario

B21. Optical fiber-based quantum communication testbeds are being setup in Sherbrooke, Montréal and Québec City, allowing QKD and other forms of quantum communications, with a goal to create open-access innovation hubs that are open to all Canadian and international partners, for the training and collaborative projects involving hardware providers, telecom operators, startups and small and medium-sized enterprises (SME), and academics	Short and medium term	Government of Québec
B22. Future plans include connecting the quantum testbeds together to allow the development of longer-range quantum communication capabilities, as well as connections to other Canadian initiatives such as QEYSSat	Medium term	Government of Québec
B23. The quantum testbeds are part of a broad vision of an integrated cybersecure advanced communications network supported by the Québec government, that involves wireless 5G/6G, AI, edge computing, and PQC technologies, as well as satellite communications	Short and medium term	Government of Québec

3. Supporting the quantum communication and PQC ecosystem

Several initiatives can be undertaken to support the quantum communication and PQC ecosystem as a whole. These initiatives will also address issues identified in the previous sections on PQC and quantum communication.

Attraction, development and retention of a quantum workforce

A diverse, skilled and large quantum workforce will be needed to support the activities described in this roadmap. This includes highly qualified personnel with scientific skills to develop advances in fundamental quantum science, technical skills to develop quantum technologies and entrepreneurial skills to bring research from the lab to the market. Quantum-literate employees, entrepreneurs and researchers, along with technicians trained in the installation, integration, operation, repair and maintenance of quantum technologies and associated components are also needed.

Partnerships and coordination between academia and industry on training will help ensure that future talent needs are met. This could include providing access to quantum technologies for students, identifying industry training needs, jointly developing curriculum and creating co-op/internship opportunities.

It will be critical for Canada to invest in developing and retaining quantum expertise, as well as accessing global pools of talent. Being internationally competitive on student, postdoctoral and industry compensation, and the work environment, will be key. In addition, there is a need to increase the number of graduates with quantum-related skills, including experts in cyber security, risk management and systems integration who have been upskilled regarding the quantum threat. Efforts must also continue in

addressing the underrepresentation of equity-seeking groups in scientific, technology, engineering and mathematics disciplines (STEM).

Talent for quantum R&D also comes from a global marketplace and bringing that talent to Canada and retaining them can be challenging. Visa timing and costs can increase the complexity of this process. Canada must make it as easy and quick as possible to bring and keep those with quantum expertise.

In December 2022, the National Quantum Strategy Secretariat held two virtual workshops led by Immigration, Refugees and Citizenship Canada which provided an overview of immigration programming and a Q&A session. More work will be needed to address this issue.

Ethical and social considerations

The broad usage of quantum communication and the migration to PQC may impact many sectors of the economy. It will be necessary to identify and address social implications and ethical considerations. This could include:

- development and export of technologies that could have dual uses in the civilian and military sectors
- the potential of quantum technologies to break widely used encryption methods with impacts on privacy and security, while encouraging responsible disclosure of vulnerabilities and ethical hacking
- equity, diversity and inclusion considerations in the quantum and PQC workforce and among those who would benefit from the technology, such as lack of access to quantum communication for remote or Indigenous communities
- inequities in the migration to PQC, leading to increased security risks among some populations, such as those least able to shoulder the costs of transition

Learning from ethical issues and regulations in artificial intelligence (AI) and other emerging technology areas and applying them to quantum technologies is key. These practices will help mitigate unintended consequences in the development of regulations. Further research on the social impacts of quantum technologies and development of an ethics framework will ensure these technologies benefit society and negative impacts are mitigated.

Programming and funding

As an emerging technology, quantum communication has different commercialization pathways than other technologies, thus requiring different supports. Quantum communication start-ups may require many years of investment before they can bring a product to market. Unfortunately, the duration of funding support offered by several federal innovation programs is much shorter than the time needed to develop quantum communication. In other cases, program requirements (such as number of employees, years since incorporation, or revenue thresholds) make it challenging to support early-stage entrepreneurs. As well, many programs are tailored towards providing loans rather than grants which is challenging for startups. Consideration of longer funding duration, follow-up investments, cash advance, and more flexible program requirements would better support the development of quantum technologies.

Access to funding through other Canadian sources, such as venture capital, angel investors, business incubators and other forms of private equity, are critical to building a vibrant quantum ecosystem, and are the largest source of funding for quantum companies. Without sufficient funding from start-up to scale-up, there is a risk that Canadian quantum companies will be acquired by foreign companies, leading to a loss of IP, talent and returns to other countries.

Intellectual property

Encouraging Canadian quantum innovators to protect and hold the rights to their intellectual property assets will stimulate growth, encourage innovation, attract investment and protect their businesses. Innovators will need to develop a global IP protection strategy.

The Canadian Intellectual Property Office (CIPO), a special operating agency of ISED, provides online Education, tools and resources and delivers IP services in Canada. Its Intellectual Property Advisors help small-and-medium sized businesses understand the value of their IP and develop an IP strategy. Information about applying for IP rights, enforcement and commercialization, as well as relevant government programs, is also available through the IP Village. Financing and tailored advisory services are available through the NRC IRAP's IP Assist program, BDC Capital's Intellectual Property-Backed Financing and ISED's ElevateIP by way of several business accelerators and incubators targeting startups. Finally, businesses can find relevant IP assets held by Canadian public sector and not-for-profit organizations through the Explore IP database where users can easily contact IP holders to discuss and negotiate a licensing arrangement.

Research security

Safeguarding Canada's quantum research and its resulting assets from foreign theft, interference, or misuse, is essential for maintaining the country's economic stability, national security, and technological advancements. Quantum research and its underlying data and resulting technologies are defined as 'sensitive research' and could be used to advance a foreign state's military, intelligence or surveillance capabilities. Sensitive research includes 'dual-use research', which refers to products, data, knowledge or technologies that have both purely scientific and military or intelligence applications. From a research security perspective, Canadian researchers may be developing or collecting knowledge or information for legitimate scientific purposes, but that information could be illicitly acquired or exploited by others, with the intent to cause harm to Canada's national interests. Unauthorized access to quantum research and technology can undermine Canada's national security interests or those of its allies, including the disruption of the economy or critical infrastructure.

The Government of Canada remains committed to protecting quantum research and technologies against foreign interference, espionage, and theft. Research security is a collective effort – researchers, academia, firms, funding organizations, and governments have a shared responsibility to identify and mitigate any potential national security risks related to research. In consultation with the science and research community, the Government of Canada has taken several measures to protect the country's world-class research and continues to provide support and guidance for implementing research security due diligence. This includes a series of federal policies, including the new Policy on Sensitive Technology Research and Affiliations of Concern, and the National Security Guidelines for Research Partnerships. Other advances that support the implementation of Canada's research security policies include the establishment of a Research Security Centre, as well as $50 million in funding through the Research Support Fund for eligible post-secondary institutions to build their research security capacity. In addition, the Government of Canada continues to release and develop new tools and resources that are available through the Safeguarding Your Research portal.

Canada is focused on ensuring that Canada's research ecosystem remains as open and internationally collaborative as possible, in alignment with its foundational principles of transparency, merit, academic freedom and reciprocity. In so doing, this enhanced posture is meant to safeguard, but not limit, Canada's cutting-edge research by mitigating research security risks.

International partnerships and agreements

No single country can succeed by doing it alone. Developing partnerships with like-minded countries will improve Canadian research and commercial outcomes. Promoting the Canadian quantum sector abroad and developing partnerships can help attract talent, secure access to global supply chains, further R&D, increase exports and advance adoption of quantum technologies. Efforts to date have included issuing joint co-operation statements with the UK and Japan, and negotiation of others is underway. As well, international missions with key markets will help Canadian companies to access new markets.

Action plan

The objective over the long-term (7+ years) is to:

- ensure that Canada has a strong talent pipeline that meets industrial needs and develops a competitive framework for the attraction, development and retention of talent
- maintain quantum training initiatives for continuous upskilling on new technology advances
- ensure that Canada is a world leader in the global trade of quantum communication and PQC products and services

The action plans below indicate short (0-3 years) and medium-term (3-7 years) actions to support the quantum communication and PQC ecosystem.

Strengthen the talent pipeline

Action item	Timeline	Lead
C1. Establish dialogue between industry and academia to identify partnership opportunities and training program needs, including number of graduates to fill industry needs	Short and medium term	Industry/Non-Profit, Academia
C2. Develop upskilling programs with industry and integrate quantum communication curricula into undergraduate, masters, polytechnic and professional programs, including hardware and component development, manufacturing and operation, including for engineers and technicians	Short and medium term	Academia
C3. Support job integrated learning and on-the-job training in quantum communication	Short and medium term	Industry/Non-Profit
C4. Undertake equity, diversity and inclusion initiatives, such as the Dimensions program and the 50-30 Challenge	Short and medium term	All
C5. Coordinate among federal, provincial and territorial governments to improve training and certification/accreditation	Short and medium term	Federal, provincial and territorial governments
C6. Strengthen the attraction and retention of talent through reviewing immigration and visa processes for quantum highly qualified personnel (HQP)	Short and medium term	Government of Canada
C7. Build Government of Canada expertise on quantum communication including on adoption and usage	Short and medium term	Government of Canada

Promote Canada's quantum communication and PQC sector domestically and internationally

Action item	Timeline	Lead
C8. Undertake outreach and marketing activities to raise awareness of quantum technologies in Canada	Short and medium term	Government, Academia, Industry/Non-Profit
C9. Establish an intergovernmental working group with representation from interested provincial and territorial governments to promote resource and knowledge sharing	Short term	Federal, provincial and territorial governments
C10. Collaborate with like-minded international jurisdictions to leverage talent, share resources and advance quantum communication R&D	Short and medium term	Government of Canada
C11. Launch international trade missions and other activities to help Canadian firms integrate into the global supply chain, improve commercial adoption, strengthen collaborations, expand into new markets and attract international talent	Short and medium term	Government of Canada

Address barriers to growth for Canadian quantum communication and PQC companies

Action item	Timeline	Lead
C12. Provide support and advice to grow quantum and PQC businesses, including entrepreneurship training, networking with quantum researchers, companies and end-users.	Short and medium term	Government of Canada, Academia, Industry/Non-Profit
C13. Connect quantum and PQC companies with funders, and encourage venture capital, angel investors, business incubators and other forms of capital to invest in the Canadian quantum sector	Short and medium term	Government of Canada, Industry/Non-Profit

Identify societal impacts and develop an ethics framework

Action item	Timeline	Lead
C14a. Identify societal impacts and develop ethics framework	Short term	Government, Academia, Industry/Non-Profit
C14b. Implement the ethics framework	Medium term	Government, Academia, Industry/Non-Profit

Protect intellectual property and improve the security posture of Canadian researchers and innovators

Action item	Timeline	Lead
C15. Advance security and IP: • governments raise awareness of security requirements, export control and IP issues among the quantum communication community • academia supports creators within academic institutions in developing IP strategies and protecting research • industry strengthens security measures, implements IP strategies and identifies challenges	Short and medium term	Government, Academia Industry/Non-Profit

Provincial actions (as submitted)

Action item	Timeline	Lead
C16. Support training, attraction, and retention of highly qualified personnel in quantum communication and cryptography	Short and medium term	Government of Alberta
C17. Leverage the GoA's CyberAlberta program to communicate and discuss quantum threat awareness material and information with Alberta's public and private organizations	Short and medium term	Government of Alberta
C18. Leverage Alberta's expertise in cryptography technologies to develop skills in quantum communication and cryptography	Short and medium term	Government of Alberta
C19. Launch and implement Alberta's Quantum Tech Framework	Short and medium term	Government of Alberta
C20. Enhance industry-academic-government collaboration to develop and protect Alberta's cyber infrastructure	Short and medium term	Government of Alberta
C21. Support work-integrated learning programs in quantum cryptography to protect Alberta's cyber infrastructure	Medium term	Government of Alberta
C22. Accelerate industry-academic collaboration in quantum communication and cryptography	Medium term	Government of Alberta
C23. Support global expansion/export of Alberta companies in quantum communication and cryptography	Medium term	Government of Alberta
C24. Attract anchor companies to Alberta to further develop and integrate the quantum ecosystem into the global value chain	Medium term	Government of Alberta
C25. Continue to develop and implement B.C.'s upskilling programs to build the quantum workforce, complementing the quantum education offered through post-secondary institutions	Short and medium term	Government of British Columbia
C26. Support increased collaboration between industry, academia, and across governments to increase access to quantum communications systems	Short and medium term	Government of British Columbia
C27. Consider creating a program that directly connects start-ups with accredited patent lawyers who can provide legal guidance and assistance in filing patents	Short and medium term	Government of Ontario

C28. Develop partnerships between quantum companies and universities to establish internships for students and attract international talent to Ontario, addressing industry needs	Short and medium term	Government of Ontario

Conclusion

Governments, academia, industry, non-profits and citizens must work together to succeed in achieving this NQS mission. That is why the Government of Canada will continue its ongoing dialogue with stakeholders, provinces and like-minded countries, and deepen its collaborations to ensure that the elements are in place for success.

Quantum communication and post-quantum cryptography are advancing rapidly. As the global context changes, Canada must remain flexible and adapt our roadmap and actions to ensure the privacy and cyber-security of Canadians in a quantum-enabled world through a national secure quantum communication network and a post-quantum cryptography initiative.