Canadian Global Affairs Institute
Institut canadien des affaires mondiales

The Quantum Revolution: Opportunities and Challenges for Canada

by Eric Miller

October 2021

POLICY PAPER

THE QUANTUM REVOLUTION: OPPORTUNITIES AND CHALLENGES FOR CANADA

by Eric Miller

CGAI Fellow
October 2021

Prepared for the Canadian Global Affairs Institute
1800, 150 – 9th Avenue S.W., Calgary, AB T2P 3H9
www.cgai.ca

ISBN: 978-1-77397-214-5

Executive Summary

The world is on the cusp of a revolution in quantum technologies. Countries and private investors around the world are deploying hundreds of millions of dollars to advance research and develop quantum technologies for defence and commercial applications.

This interest is driven by what quantum technologies can do relative to their "classical" counterparts. Quantum technologies function by harnessing the key characteristics of the theory of quantum mechanics, including superposition, entanglement and uncertainty. The resulting technologies are expected to be diverse and far reaching. For example, quantum computers are expected to overcome most "public key encryption" systems, presaging a radical change in cybersecurity. Given its aptitude for navigating complexity, quantum tools are expected to shave years off the time to market for medicines. Secure, efficient communications among drones and other autonomous vehicles will underpin safety and operational effectiveness in the crowded skies of the future. Of course, these nearer terms examples will be joined by applications barely yet imagined as the technology matures.

The competition for quantum supremacy is growing more intense by the day. China has been heavily focused on quantum for over a decade and is among the most ambitious in pursuing these technologies. It is known to have made strong advances in quantum communications among other areas. Watching China's success in transmitting quantum encrypted communications via satellite, the United States began seriously investing in quantum in 2018. Significant government and venture capital is now flooding into a vast array of applications. The United Kingdom, Europe and Japan are similarly making significant investments.

Canada enters the quantum era extraordinarily well positioned. It spent over a C$1 billion in the decade-plus prior to 2018 building out a world class research and commercial ecosystems. Strong centers of excellence include Vancouver, Calgary, Waterloo, Toronto, and Sherbrooke. These centers are developing strong local research and commercial partners as well as linkages with global players. The C$360 million investment announced by the federal government in the spring of 2021 and the development of a National Quantum Strategy will significantly advance this work.

In its final section, the paper offers some recommendations on how Canada should build on its carefully nurtured advantages in quantum. The key thematic areas in which it offers recommendations include: (1) securing national economic advantage; (2) advancing national security; (3) pursuing international cooperation; and (4) developing infrastructure for the quantum era.

Quantum computing really stands out as having exponentially greater power … (meaning) that on any future time scale, it's just going to dwarf anything else … (Y)ou get an exponential advantage using a quantum computer which really turns the impossible into the possible.

- Jeremy O'Brien, CEO of PsiQuantum (2019)[1]

In August 2016, China launched its QUESS satellite into orbit with the explicit objective of using it to transmit quantum encrypted communications. This was to be the backbone of "Project Jinan," which saw an experimental quantum communications network built in the city of Jinan – located partway between Beijing and Shanghai. A few months later, a test was initiated. China successfully transmitted a green laser beam comprised of entangled photons via satellite between two ground stations 750 miles apart. Technically, this was an extraordinary achievement. The fragile nature of quantum particles makes them very hard to transmit. Previous ground-based experiments using optical fibre found that the signal would get corrupted after just 150 miles.[2] While this may sound like an interesting science project, it actually was the foundation of what many see as the world's first unhackable communications network. China's success in satellite transmission garnered worldwide attention and analysts began to speak of the "age of quantum cryptography."

In Washington and other Western capitals, Project Jinan was a wake-up call. For the first decade and a half of the 21st century, U.S. attention was centred on fighting terrorists from Mesopotamia to the Hindu Kush. Less emphasis was therefore placed on building the next generation of advanced technologies necessary to confront sophisticated adversaries. As Diana Franklin, director of computer science at the University of Chicago, told Congress in May 2018, "gaps in funding (over the past 15 years) have left the U.S. scrambling to stay ahead in quantum (technologies)."[3] By contrast, each year of the 21st century, China was ramping up its technology investments as its strength grew militarily and economically. This included pouring billions of dollars into mastering quantum technologies.

As the full scope of China's rise was settling into the minds of policy-makers, the prospect of facing an adversary with a substantially unhackable communications network pushed the United States to seriously enter the quantum game. At the same time, policy-makers began to see that the ability to master quantum phenomena would provide a foundation for significant economic opportunities. The U.S. passed its organizing legislation, the *National Quantum Initiative Act* (NQI), in 2018. Concurrently, jurisdictions such as Japan, Germany, India and Russia are spending heavily on developing their own capabilities for their own purposes.

---

[1] Chris O'Brien, "Interview of the Week: Jeremy O'Brien," The Innovator, January 13, 2019, https://innovator.news/interview-of-the-week-jeremy-obrien-9d5755dc4483.
[2] Sophia Chen, "Chinese Satellite Relays a Quantum Signal between Cities," *Wired*, June 15, 2017, https://www.wired.com/story/chinese-satellite-relays-a-quantum-signal-between-cities/.
[3] Diana Franklin, Testimony for Subcommittee on Digital Commerce and Consumer Protection, House Committee on Energy and Commerce, May 18, 2018, https://docs.house.gov/meetings/IF/IF17/20180518/108313/HHRG-115-IF17-Wstate-FranklinD-20180518.pdf.

It is hard to accurately predict the full scope of technologies that advances in quantum will yield. Quantum computing is receiving most of the attention as tech giants and emerging players race to build devices to apply quantum phenomena to storing and processing data. Various groups are presently experimenting with applications in areas as diverse as accelerating drug development to optimizing supply chains. A parallel intensive effort is underway in quantum communications, which links computers through a new internet built on quantum principles. The United States has publicly committed to build a national quantum internet by 2030, even as China is advancing rapidly in this area.

In addition to the infrastructure and methodologies to enable data transmission, areas of inquiry such as quantum key distribution are moving ahead. Quantum metrology, which uses quantum phenomena to undertake highly precise measurements, is making strides in areas such as biological imaging and simulation. Quantum sensors are being developed for applications ranging from precisely mapping targets to mineral exploration. This big and diverse array of quantum applications will drive many tangible innovations.

Cyber-security is an overarching theme for researchers in the quantum age, including the arcane but crucially important area of cryptography – the study of the use of codes to facilitate secure communications. Communications experts have a strong theoretical understanding of how quantum computers will be able to crack most existing public key cryptographic systems. In other words, quantum computers will render largely useless most of the existing encryption systems that are used to secure our data, from credit cards to passports to sensitive emails. While quantum computers have yet to achieve the power and accuracy necessary to break widely used encryption methodologies such as RSA (Rivest-Shamir-Adleman), it is only a matter of time until the arrival of what some security experts call "Q Day."[4] In preparation, some researchers and government agencies are turning their attention to creating quantum encryption algorithms and to addressing foundational elements in areas such as true randomness. The U.S. National Institute of Standards and Technology (NIST), for example, has been running an open international competition to design "post-quantum algorithms."[5]

Canada has been an early investor in quantum. As quantum applications prepare to transition from the laboratory to the marketplace, Canada's work in nurturing world-leading research centres and innovative start-ups seems poised to pay off. However, the quantum innovation game is getting harder and more intense. In order to benefit, Canada needs to focus on at least three areas: (1) growing great quantum companies; (2) supporting research that maximizes Canadian participation in breakthrough quantum innovations; and (3) preparing public institutions (both civilian and military) and national infrastructure for the quantum age. Ottawa announced a significant new investment in its April 2021 budget. The key question now is around execution.

[4] RSA is a widely used asymmetric cryptography algorithm, using a public key for encrypting messages and a private key for decrypting them. The RSA algorithm hinges on the difficulty that classic computers have had in factoring very large numbers. Quantum computers are expected to overcome the current prime factorization challenges, leaving communications among computers largely exposed. The day when RSA and similar algorithms are definitively overcome is referred to as Q Day.

[5] "Post-Quantum Cryptography," National Institute of Standards and Technology, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

Quantum is a complex area. Part 1 of this paper will therefore explain what quantum technologies are and how the sector has evolved. Part 2 will offer some examples of how quantum technologies are likely to be applied in military, commercial and hybrid settings. Part 3 will elaborate on what major jurisdictions are doing in quantum, including China, the United Kingdom, Europe, Japan and the United States. Part 4 will describe the Canadian context and Part 5 will offer recommendations for how to retain and extend Canada's leadership position in the quantum revolution.

What are Quantum Technologies?

The quantum revolution has been more than a century in the making. The word "quantum" is the singular form of the Latin adjective "quantus," meaning "how much." Quantum technologies are based on quantum mechanics, a fundamental theory in physics that describes the physical properties of nature at the scale of atoms and sub-atomic particles.

The ideas that gave rise to quantum mechanics arose gradually, building especially on the work of Max Planck, Marie Curie and Albert Einstein, in the first decades of the 20th century.

Quantum mechanics is one of the strangest, most magnificent and least intuitive theories ever to be developed in the history of science. While studying atoms and sub-atomic particles sounds esoteric, in the decades after it was proposed, knowledge of quantum mechanics would facilitate the development of technologies as diverse as the atomic bomb, the semiconductor, life-saving magnetic resonance imaging (MRI) machines, and global positioning systems (GPS). Quantum physics would also set off fierce philosophical debates about the nature of God and the interconnectedness of the universe.

In 1913, visionary Danish physicist Niels Bohr proposed the core foundations of what become the theory of quantum mechanics. In a quantum world, the universe does not unfold in a predictable, linear fashion. Rather, the future is merely probabilistic. Over the next decade and a half, Bohr and contemporaries, including Werner Heisenberg, Erwin Schrödinger and Max Born, refined quantum mechanics into a fulsome theory.

Einstein, whose theory of relativity opened the door, led the charge against quantum mechanics, famously stating that "God doesn't play dice with the universe." His 1935 paper with Boris Podolsky and Nathan Rosen, which became known as the EPR Paradox, argued that the description of physical reality by quantum mechanics was incomplete.

It would take decades of experimentation to resolve this debate. In 1964, John Bell, an Irish physicist, developed a way to test Bohr's and Einstein's ideas. As he wryly summed up his conclusions: "Bohr was inconsistent, unclear, willfully obscure and right. Einstein was consistent, clear, down-to-earth and wrong."[6]

Broadly speaking, physicists seek to describe the nature of the universe. When they are successful, engineers can then build tools and systems that harness these underlying dynamics to solve real-world problems. Bell's tests were instrumental in further solidifying quantum theory. In 1984, a Canadian, Gilles Brassard, professor at the Université de Montréal, co-invented BB84, a protocol for leveraging quantum mechanics for cryptography. This provided a key theoretical foundation for quantum computing. In the late 1990s, the first rudimentary quantum computers were built. Some 20 years later, quantum computers have achieved supremacy over the best supercomputers in certain experiments. Over the next few years, this advantage will become more consistent and facilitate the movement of quantum computers from the laboratory into the outside world. Concurrently, a whole new array of other quantum technologies will similarly transition.

One key difference between the quantum technologies to come and first-generation 20th century technologies, such as semiconductors and GPS systems, is that the latter benefited from quantum knowledge but did not "directly harness uniquely quantum phenomena such as superposition, uncertainty or entanglement within individual quantum states to perform a task or achieve a result."[7] The second-generation applications are built squarely on manipulating quantum effects to achieve outcomes.

Meet the Quantum Computer

Of all the areas of quantum technologies, computing is receiving the most attention. So, how is a quantum computer different from the classical computer we use today?

Classical computers store information through electrical voltage based on binary digits or bits: either zero for a low charge or one for a high charge. To use an analogy, one flips a coin and it is either heads or tails. By contrast, quantum computers store information in qubits, which exhibit physical properties rooted in quantum phenomena, including the direction of an electron's spin – either up or down. A key difference is the phenomenon in quantum mechanics known as superposition, in which an electron can exist in two separate quantum states simultaneously. In other words, qubits can essentially be both zero and one at the same time.

In practical terms, a system with multiple qubits has many more combined possible values than a system with an equal number of bits. For example, a three-bit traditional computer can hold up to eight possible values. A three-qubit system can hold up to 256 possible values. As Michael Morris, CEO of Topcoder, notes: "Instead of solving one problem at a time … quantum computing … can solve thousands of problems at the same processing speed, with the same processing

[6] Graham Farmelo, "Random Act of Science," *New York Times*, June 11, 2010, https://www.nytimes.com/2010/06/13/books/review/Farmelo-t.html.
[7] Andrew Fearnside, "Mapping the Commercial Landscape for Quantum Technologies," *Physics World*, December 3, 2018, https://physicsworld.com/a/mapping-the-commercial-landscape-for-quantum-technologies/.

power."[8] This means that accurately gauging the outcome of complex multivariable problems with which conventional computers struggle will now become possible.

Another principle of quantum mechanics that defines the difference between traditional and quantum computers, particularly as it relates to communications between computers, is entanglement. Quantum entanglement can be defined as a physical phenomenon that occurs when a group of particles are generated, interact or share spatial proximity in such a way that the quantum state of each particle cannot be described independently of the others, including when separated by a large distance. Quantum messages sent from one computer to another are thus transmitted as entangled particles.

Illustration 1

Source: Scott Adams, Dilbert[9]

Still another key element of quantum mechanics is Heisenberg's Uncertainty Principle, which argues that it is impossible to measure the position and velocity of a particle at the same time. Applied to quantum computing, this principle says that it is impossible to observe a stream of entangled particles carrying a message from one quantum computer to another without altering it. In other words, the interception of messages, which is relatively simple on a classical computer, becomes nearly impossible on a quantum computer. Intercept attempts between two quantum computers trigger error messages that are transmitted to the sender and receiver.

Quantum computers also have a clever way to solve the eternal challenge of any communications system: security at the end points. Unique keys are distributed to the originator and addressee(s) of a message via quantum teleportation. This allows users to transmit and unlock messages without others seeing them. Many experts argue that such quantum key distribution (QKD) is the linchpin that will make quantum computers substantially unhackable.

[8] Maria Korolov and Doug Drinkwater, "What is Quantum Cryptography? It's No Silver Bullet, But Could Improve Security," CSO, March 12, 2019, https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.html#:~:text=Quantum%20cryptography%2C%20also%20called%20quantum,outside%20of%20the%20intended%20recipient.
[9] Scott Adams, "Dilbert Cartoon" printed in "The Basics of Quantum Computing," Quantum Inspire, https://www.quantum-inspire.com/kbase/introduction-to-quantum-computing/.

Table 1

Milestones in Quantum Computing: 1998-2021

1998	• IBM, Oxford, Berkley, Stanford, MIT build a two-qubit system.
2000	• Los Alamos National Laboratory builds a seven-qubit quantum computer.
2006	• University of Waterloo's Institute for Quantum Computing, Perimeter Institute for Theoretical Physics and MIT build a 12-qubit system.
2008	• Vancouver's D-Wave Systems builds and successfully sells a 28-qubit computer.
2017	• Large tech companies join the quantum race. IBM unveils a 50-qubit system. • China's Project Jinan experiments with sending quantum encrypted information from one ground station to another via satellite.
2018	• Google unveils a 72-qubit system. • U.S. *National Quantum Initiative Act* becomes law.
2019	• U.S. rolls out detailed national co-ordination infrastructure for all aspects of its quantum efforts. • Google announces its 53-qubit system has achieved "quantum supremacy," solving a problem in 200 seconds that it would take a conventional supercomputer many years to complete. Critics point to "noise" and fidelity problems.
2020	• Proof-of-concept quantum radar announced. • Maryland-based Ion-Q announces a 32-qubit quantum computer with 99.9 per cent fidelity. • Vancouver-based D-Wave announces a 5,000-qubit computer, affirming that its quantum annealing technology can scale. • Researchers in the U.K. report building an eight-user, city-scale quantum network in Bristol. • The U.S. releases a detailed blueprint for building a national quantum internet within a decade.

	• AWS launches Braket, which allows customers to build and test quantum algorithms on various types of quantum computers, including quantum annealers (D-Wave), gate-based ion trap processors (Ion-Q) and gate-based superconducting processors (Rigetti). • Chinese researchers claim to have achieved quantum supremacy, using a 76-qubit integrated photonic system, which performed calculations at 100 trillion times the speed of classical supercomputers.
2021	• Chinese researchers report building the world's largest integrated quantum communications network, combining over 700 optical fibres with two QKD-ground-to-satellite links for a total distance between nodes of up to 4,600 km. • Researchers in China report the successful transmission of entangled photons between drones, marking the first case in which entangled particles were sent between two moving devices.

There are, of course, still ample technical and human risks that will create cyber-security vulnerabilities. Nevertheless, the level of structural security embedded in quantum computers is vastly greater than anything imaginable with classical computers and today's internet.

The quantum computing industry has three main challenges to substantially address before quantum computing can be viably commercialized at something approaching scale. These are:

1. To make their systems more powerful. In other words, companies are seeking to increase the number of qubits embedded in their computers;
2. To increase the degree of accuracy of the information produced. Given the probabilistic nature of the outputs generated by quantum computers, the ability to ensure fidelity and identify and correct errors is essential; and
3. To increase both the demonstrated practical applications and user-friendliness of quantum computers.

Researchers are making strides in each of these areas.

There are various estimates about the probable speed of adoption of quantum computers and the resulting market size over the medium term. For example, a 2020 estimate by Research and Markets sees the global quantum computing and communications markets reaching US$65 billion by 2030, up from US$500 million in 2019.[10] On the adoption side, Gartner research found

[10] Research and Markets, "Quantum Computing Market Research Report," Intrado Globe Newswire, April 2020, https://www.globenewswire.com/news-release/2020/04/06/2011932/0/en/Worldwide-Quantum-Computing-Market-2019-to-2030-Drivers-Restraints-and-Opportunities.html.

that 20 per cent of Fortune 500 companies will budget for quantum projects by 2023, up from less than one per cent today.[11]

A key question related to scaling is to what extent there is a standardization or interoperability of systems. Creating a powerful, accurate quantum computer is a complex process. Physicists, chemists and computer scientists are experimenting with a wide variety of techniques for manipulating the particles necessary to deliver the desired effects. Broadly speaking, there are presently two major approaches: systems that use quantum annealing and systems that use gates. Canada's D-Wave has arguably been the most commercially successful pure-play quantum computing company. It is virtually alone in using quantum annealing. Critics long argued that its methodology is not scalable, but it is proving the critics wrong thus far. The other contenders use gates, but differ fundamentally in specific technique, whether integrated photonics, ion trapping or superconducting circuits. In short, companies are simultaneously trying to define the best architecture and to engineer it. This is the ultimate in high stakes in the technology business.

For those focused on producing software for quantum computers, hardware agnosticism (i.e., the ability to run on everyone's platform) is the name of the game. The COVID-19 pandemic has also pushed quantum companies to refine their remote, cloud-based connectivity.

Amazon Web Services (AWS) has emphasized its customers' ability to access different types of quantum computers built on distinct methodologies. In August 2020, AWS launched Braket[12] – a fully managed quantum computing service that helps researchers and developers explore potential applications on their preferred type of quantum computer. AWS has agreements with D-Wave (quantum annealing), Ion-Q (gate-based ion trap processors) and Rigetti (gate-based superconducting processors). Each of these systems has its strengths and weaknesses. With cloud-based access to all three systems, AWS customers can apply design and test quantum algorithms on the hardware of their choice as they optimize their understanding of how quantum can solve their key problems.

By providing access to these different systems, AWS has played to its strengths as the world's most widely adopted and comprehensive cloud computing platform. In short, it is positioning to power whatever the winning quantum technologies are. Customers are going to AWS to work through a variety of business problems in the Braket environment. For example, BMW recently announced a collaboration with AWS through its Quantum Solutions Lab to crowd-source solutions to a number of challenges using quantum computing. These range from optimizing the positioning of sensors in the car for collision avoidance to automating quality assessments.[13] Such initiatives, in which different quantum methodologies are assessed and compared for their application to

---

[11] Susan Galer, "Quantum Technology 2020 Trends: These are the Immediate Security Threats and Opportunities," *Forbes*, February 13, 2020, https://www.forbes.com/sites/sap/2020/02/13/quantum-technology-2020-trends-these-are-the-immediate-security-threats-and-opportunities/?sh=daaad846ac21.
[12] Staff, "Quantum Computing is Now Available on AWS through Amazon Braket," Amazon.com., https://aws.amazon.com/about-aws/whats-new/2020/08/quantum-computing-available-aws-through-amazon-braket/.
[13] Martin Schuetz and Jordan Con, "Exploring Industrial Use Cases in the BMW Group Quantum Computing Challenge," AWS Quantum Computing Blog, July 13, 2021, https://aws.amazon.com/blogs/quantum-computing/exploring-industrial-use-cases-in-the-bmw-quantum-computing-challenge/.

different problems, will be useful for expanding knowledge about what annealing, ion traps and superconducting circuits are best used for.

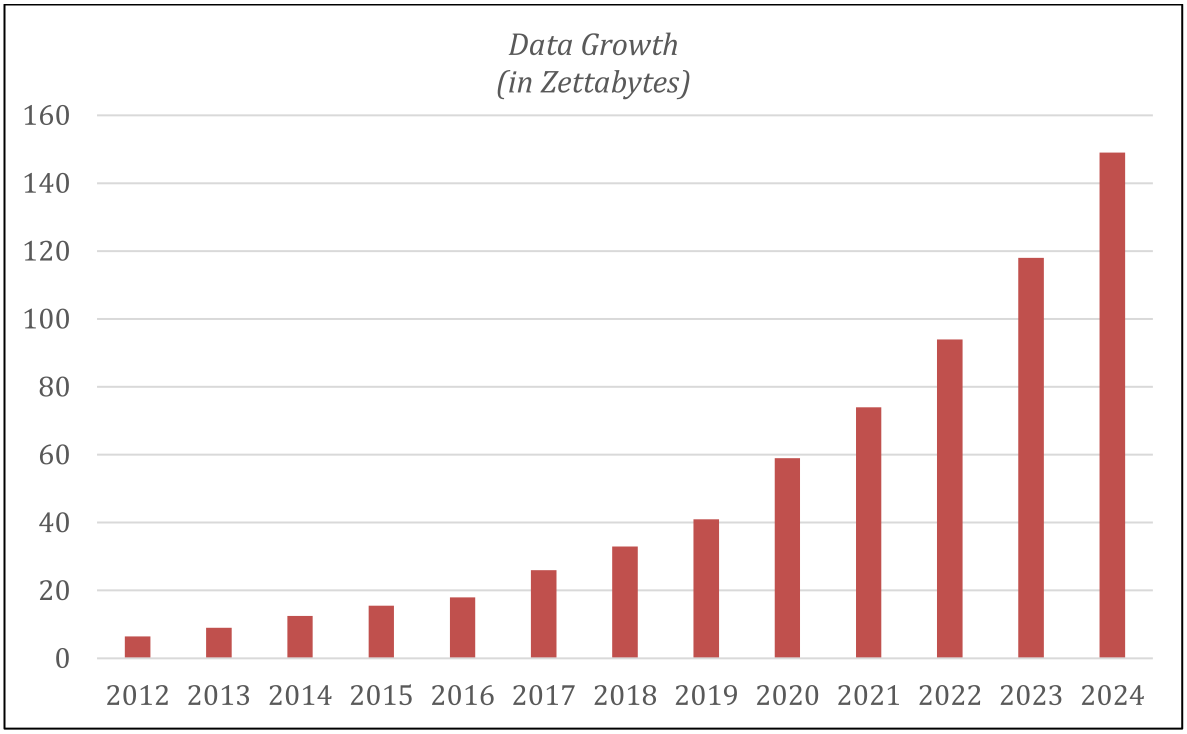
While much of the activity today is focused on understanding how quantum computers work and what they are best used for, at some point soon the question of when we might expect mass market adoption will be asked. Given the growing demand for computing power, it cannot come soon enough. The computer industry has found it challenging to continuously increase both the power and miniaturization that customers want. Moore's Law, which dates from the 1960s, posited that computing power would double every two years, but Moore's Law began to break down in the early 2000s. The semiconductor industry now has to invest increasing amounts of money to squeeze out further incremental growth in computing power.[14] Concurrently, the world is going through a data explosion as the Internet of Things (IoT) becomes truly ubiquitous and people spend ever more of their lives online. According to Statista, the world created, captured, copied and consumed some 18 zettabytes of data in 2016. This rose to 59 zettabytes in 2020 and is expected to hit 149 zettabytes in 2024.

As noted above, the probabilistic nature of quantum computers will make them massively more powerful without the constant challenge of shrinking and cramming ever more capacity into each integrated circuit that conventional computer-makers face. One key engineering challenge, at least initially, is that some of the leading quantum computers require a "fridge" – an ultra-cool environment that allows electrons to spin without distortion. Optimizing cloud-based solutions that allow users to connect quantum computers remotely is essential.

[14] See Victoria Coleman's presentation at the Woodrow Wilson Center session entitled "When the Chips are Down: Navigating Strengths and Strategic Vulnerabilities in the Semiconductor Industry," Wilson Center, March 10, 2021, https://www.wilsoncenter.org/event/when-chips-are-down-navigating-strengths-and-strategic-vulnerabilities-semiconductor-industry. (Starts at 6:45 of the video). Moore's Law is attributed to Gordon Moore, who observed in 1965 that the number of transistors in a dense integrated circuit doubles every two years.

Chart 1

Volume of Data Created, Captured, Copied and Consumed Worldwide: 2010-2024[15]



Source: Statista

What Will Quantum Technologies Do?

The arrival of quantum technologies will be transformative in a whole array of sectors. It is not an overstatement to assert that the difference between a conventional computer and a quantum computer will be as radical as the shift in transportation modes in the early 20th century from the horse to the automobile. While quantum computers are at the forefront, quantum communications systems, sensors, radar, ultra-precise atomic clocks and other applications will transform our world. As with any emerging set of technologies, it is hard to know with any certainty what their full impacts will be. After all, innovations tend to build on each other. This section provides some examples of how it will affect specific areas.

Military

Many analysts posit that the world's major powers are entering a "new revolution in military affairs" that is underpinned by an array of scientific advances, including hypersonics, artificial

[15] Statista, "Volume of Data/Information Created, Captured, Copied and Consumed Worldwide: 2010-2025," https://www.statista.com/statistics/871513/worldwide-data-created/#:~:text=The%20total%20amount%20of%20data,ever%2Dgrowing%20global%20data%20sphere.

intelligence, autonomous systems, ubiquitous sensors and quantum technologies.[16] Of these advancements, quantum could have the farthest reaching impacts.

Two examples of how quantum will underpin the future of warfare are:

- Quantum sensing: The Department of National Defence's Quantum Science and Technology Strategy identifies quantum sensing as a priority.[17] Canada has good technological foundations in quantum sensing and has identified this as its lane of choice among key security partners. Sensing will be hugely important both for awareness of the functioning for specific systems as well as knowledge of the shifting battlefield configurations. For the most part, quantum sensing is at the laboratory prototype stage. The quantum-based gravimeter is a good example of what is to come. It has a level of precision five orders of magnitude higher than the best classical gravimeter. This allows for a detailed mapping of the Earth's surface and underground at a resolution of one centimetre. The potential for this technology is vast. In a military context, it will be ideal for detecting tunnels or objects behind walls. The biggest near-term challenge to deployment is the miniaturization of the laser apparatus used for cooling atoms, although progress is reportedly being made.[18]

- Another emerging sensing application is stealth-defeating radar. Defence Research and Development Canada is working with partners to develop this technology which uses a technique called quantum illumination. When refined and deployed, quantum radar will be able to detect objects that are smaller, faster and further away, all while being less detectable and less subject to jamming.[19] This type of transformative radar will become particularly important as drone technology proliferates.

- Secure communications among autonomous drones/vehicles: One strength of quantum computers is that they can perform multiple complex calculations with different scenarios simultaneously. In January 2021, China flew a pair of drones in formation, communicating with and between them via a quantum encrypted communications channel. Their operations were managed by two ground stations one kilometre apart. Autonomous vehicles, whether airborne or terrestrial, need to constantly communicate with each other and the ground all while watching for threats and focusing on the target. Quantum computers have the heft to handle such complex simultaneous tasks. Moreover, the communications are secure. As noted above, operators can tell if entangled photons are being intercepted. This experiment offers important insights about how to operationalize

[16] Christian Brose, "The New Revolution in Military Affairs," *Foreign Affairs*, May/June 2019, https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs.
[17] Department of National Defence, "Quantum S&T Strategy: Preparing for Technological Disruptions in the Future Operating Environment," Government of Canada, January 2021, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/dnd-caf-quantum-science-and-technology-strategy.html.
[18] Michael Krelina. *Quantum Warfare: Definitions, Overview and Challenges*. Czech Technical University. March 24, 2021. https://arxiv.org/abs/2103.12548. Krelina is CEO of Quantum Phi.
[19] Institute for Quantum Computing, "Quantum Illuminates Potential for New Radar Technology," University of Waterloo, March 18, 2019, https://uwaterloo.ca/institute-for-quantum-computing/news/quantum-illuminates-new-potential-radar-technology.

the advantages of quantum communications for real-time military operations and points to the future of air power.[20]

Civilian

The impact of quantum technologies on the civilian side will be similarly vast. Some applications already taking shape are:

- Authentication: This is one of the greatest challenges facing the global economy. The process of proving whether a product is genuine or some kind of fake is time-consuming and relatively crude. The cost of counterfeit goods to the global economy runs in the hundreds of billions of dollars per year. A number of research institutions and companies are experimenting with using 2-D materials such as graphene as a unique quantum scale identifier – or Q-ID.[21] By applying quantum technology, everything from airplane parts to designer handbags to medicines could be tagged with a 2-D material identifier that government authorities or consumers could verify.[22] Some experiments are focusing on ways to use smartphones to do the authentication. In 2020, researchers at the University of Waterloo announced that they had developed a prototype of a photonic crystal mirror that would enable users to detect counterfeit currency.[23] By using quantum technology, consumers, brand holders and governments have the potential to put fraudsters significantly on the defensive.

- Imaging: Researchers are making extraordinary progress in quantum imaging. A few innovative cameras are on the market or under development. This includes cameras that can take accurate pictures in almost complete darkness. One promising area in this field is quantum holography. Classical holography creates two-dimensional renderings of three-dimensional objects with a laser beam split into halves. Holographs are already used for credit card and passport security and in areas such as medical imaging. In a classical scenario, the holograph is created by measuring the differences in the light's phase where the two beams meet. The quantum holography process also uses a laser beam split into two paths, but, unlike in classical holography, the beams are never reunited. Instead, the process harnesses the unique properties of quantum entanglement to gather the coherence information required to construct a holograph.[24]

---

[20] Sam Jarman, "Quantum Connection is Made by Flying Drones," *Physics World*, January 23, 2021, https://physicsworld.com/a/quantum-connection-is-made-by-flying-drones/.

[21] Graphene is a material of carbon atoms one layer thick that is arranged in a honeycomb structure. It has been used for everything from ultra-high frequency communications to boosting battery performance. It is now being used in the creation of unique quantum-scale identifiers. Creators of these tags configure single atoms in unique ways that are almost impossible to clone. The tags can be read with a smartphone, allowing anyone to see whether a product is the genuine article.

[22] Abby Norman, "New Quantum Technology Lets You Use Your Phone to Identify Counterfeit Goods," *Futurism*, July 5, 2017, https://futurism.com/new-quantum-technology-lets-you-use-your-phone-to-identify-counterfeit-goods.

[23] Institute for Quantum Computing, "New Mirror Made for Quantum Research Could Catch Counterfeit Cash," University of Waterloo, April 13, 2020, https://uwaterloo.ca/institute-for-quantum-computing/news/new-mirror-made-quantum-research-could-catch-counterfeit.

[24] University of Glasgow, "Holography 'Quantum Leap' Using Entangled Photos Could Revolutionize Imaging," Sci-Tech Daily, February 12, 2021, https://scitechdaily.com/holography-quantum-leap-using-entangled-photons-could-revolutionize-imaging/.

- Precision Chemistry: Quantum technologies are poised to empower precision chemistry. Take, for example, the development of new medicines. At present, the development lead times for new drugs is measured in many years. Scientists need to work to understand the exact structure of molecules and how they interact with other molecules in certain environments. It is nearly impossible to accurately model these complex interactions using conventional computers. Researchers are therefore forced to undertake repeated optimization cycles that are expensive and time-consuming. Quantum computers are ideally suited to capture, synthesize and assess the dynamic effects of large amounts of disparate information. In future, researchers will be able to run optimization cycles digitally and to deploy the resulting formulations to the real world with a high degree of confidence.

- Optimizing Supply Chains: One of the most famous challenges in mathematics is the travelling salesman problem (TSP). The TSP asks: "Given a list of cities and the distances between each pair of cities, what is the shortest possible route that visits each city exactly once and returns to the origin city?" As many have learned during the pandemic, supply chains are complex and are subject to many TSP-like challenges. Major multi-brand retailers stock thousands of products from hundreds of suppliers. Key questions include: Where to source from? How to route shipments? Where to locate warehouses? How to organize shipments to stores? These are all classic optimization problems on which quantum computing thrives.

- Providing the Computing Power to Allow Artificial Intelligence (AI) to Learn: AI is undergoing its own significant advancements in parallel with quantum. In order to reach their full potential, AI systems need the type of robust computing power that quantum systems enable. Take the case of intelligent autonomous vehicles. Quantum will play an important enabling role. To be scalable, the vehicle must learn to read the road and traffic conditions and to be able to make good driving decisions under specific circumstances. This includes everything from knowing how to swerve when a pedestrian suddenly appears to adjusting driving style in winter. Even under normal circumstances, the vehicle must learn to accelerate/decelerate, turn and go around other vehicles. These are complex tasks. AI systems, like regular drivers, will learn these tasks over time. Quantum computers will speed the knowledge acquisition and adoption process.

Hybrid

- Transforming Cyber-security: When there is a major advance in technology, there tend to be significant ramifications in many areas. Quantum computing is certain to bring a myriad of changes defensively and offensively in the area of cyber-security.

On the defensive side, some analysts have hailed the near-term arrival of quantum computing as a solution to the vulnerabilities in existing digital networks. For example, quantum has the potential to significantly enhance the quality and robustness of digital identity. With respect to communications between computers, quantum entanglement and quantum key distribution will make it significantly harder for those seeking to intercept or alter quantum encrypted communications. In truth, there is no unhackable network. Given the many cyber-attacks generated by human negligence or maliciousness, technical solutions alone cannot solve this problem.

Offensively, quantum computers have the potential to break any existing public key encryption system that a classical computer uses. Current encryption systems, including the much-applied RSA algorithm, tend to rely on the mathematical idea of prime factorization. In practical terms, it works on the assumption that no computer can efficiently decrypt the encryption equation in any reasonable timeframe. With quantum computers, this could change within a decade. In fact, Shor's algorithm, the theoretical foundation for overcoming prime factorization, is already well known. This would render ineffective much of the existing computer security architecture. The U.S. government and others are therefore hard at work designing post-quantum algorithms for encryption.

To understand the significance of these vulnerabilities, consider the fact that the adoption of technology tends to be much slower than its development. Organizations that adopt quantum computers will do so gradually, often after considering what problems quantum means could best tackle. During the hybrid phase between when quantum computers first become widely available but sit alongside classical computers, attackers with quantum capabilities will be well positioned to inflict harm on companies whose networks, industrial control systems, ATMs, digital payment infrastructure and other tools are adapting to a quantum world. Management consultancies have already started to encourage companies to embrace crypto agility.[25] In other words, firms should start thinking about the quantum transition now, including how it will be handled and what infrastructure will need to be updated or replaced.

The current epidemic of ransomware attacks underscores the scale of the problem. Considering how many otherwise sophisticated companies and organizations have weak cyber-security even after years of attacks and media stories about the risk, one cannot be especially optimistic about the speed at which organizations will become agile.

One esoteric but important implication of the transition from classical to quantum architecture is that significant amounts of new software will be required. Almost inevitably, mistakes will be made. In skilled hands, these errors form the foundations of new zero-day exploits which can be directed to power cyber-attack tools.[26] In the aftermath of the May 2021 Colonial Pipeline ransomware attack, the Biden administration released an executive order, Improving the Nation's Cybersecurity.[27] It includes a major focus on software integrity. It remains to be seen how this will

[25] Accenture, "The Race to Crypto Agility," 2021, https://www.accenture.com/_acnmedia/PDF-145/Accenture-Crypto-Agility-POV-v7-0.
[26] A "zero day vulnerability" is a flaw in software or hardware of which its developers are not aware. It has thus been zero days since the flaw has been detected and patched. Attackers can exploit or weaponize these vulnerabilities to penetrate systems for purposes ranging from theft to sabotage; hence the term "zero day exploit." See Nicole Perlroth, *This is How They Tell Me the World Ends*, (London: Bloomsbury, 2020) for a detailed overview of the creation and application of cyber-weapons.
[27] Government of the United States, "Improving the Nation's Cybersecurity," Executive Order, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

apply in practice, including what its impact will be on the integrity of software developed for quantum systems.

An additional set of quantum cyber-security implications affects international diplomacy. It is widely known that intelligence agencies are stockpiling a wide array of communications and documents that they have yet to figure out how to decrypt. As quantum computers become more powerful and widely available, some of this information, which its originators have gone to great lengths to conceal, is likely to become accessible. One can only begin to imagine the information that will be released to the world and its implications for international relations, security and the global economy.

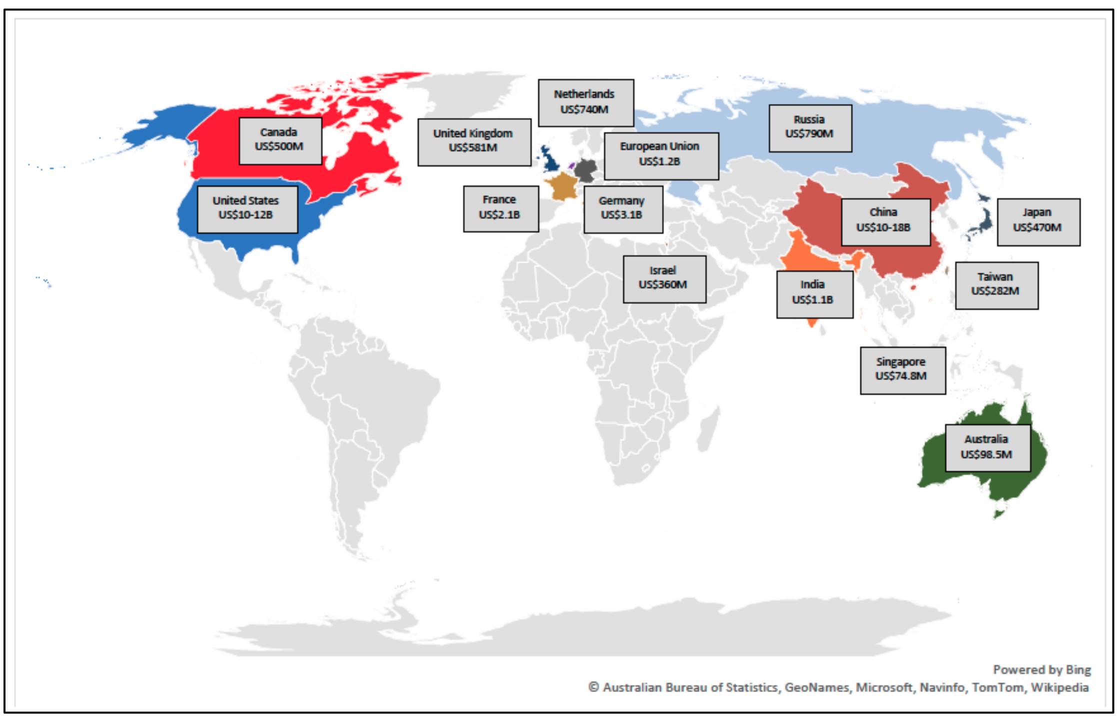
What Are Major Countries Doing?

Around the world, governments and the private sector are starting to invest significantly in quantum. Graph 2 provides an overview of the breadth of nations investing in quantum technologies. Even assuming the lower estimates for the United States and China, public-sector expenditures through 2025 are expected to exceed US$30 billion. Notably, this largely excludes additional classified investments by defence and intelligence organizations.

Illustration 2

Estimated Public-Sector Investments in Quantum: 2018-2025

(Countries whose expenditures exceed US$50 million in the target period)



Many countries have set and funded their quantum programs to run until the mid-2020s. The above illustration (Illustration 2) is intended to capture ongoing, publicly announced public-sector expenditures. It does not reflect pre-2018 expenditures, which, in many cases, established the research and commercial infrastructure on which countries are now relying. For example, Canada spent well over US$1 billion between 2000 and 2018, establishing and supporting research centres and nurturing companies. Canada's expenditure number is intended to capture headline federal and provincial contributions, including grant renewals.

Illustration 2 also excludes private-sector investments. For example, five of the top firms in quantum computing – PsiQuantum, D-Wave, Rigetti, Ion-Q and Cambridge Quantum Computing – have already received well over US$1 billion in VC funds.[28] These are not reflected in the U.S., Canadian and U.K. national numbers. In total, according to PitchBook, investors poured US$779.3 million into 77 quantum computing deals in 2020, including US$557.5 million into U.S. and Canadian quantum computing companies.[29]

Assembling a comprehensive list of public-sector expenditures is challenging. China is the most difficult to estimate, given its lack of budgetary transparency in this space. The figure of US$10 billion is cited regularly in articles about China's quantum efforts, but there is no agreement on the duration of these expenditures and no link to a primary source. The range set forth in Illustration 2 for China represents a best guess for what is known about its quantum program and what it would likely cost. Putting spending estimate challenges aside, what are the major players doing with their quantum investments?

Table 2

China: Five Years of Quantum Achievements

August 2016: Launch of first quantum satellite (QUESS).

June 2017: First quantum-based transmission between two ground stations via satellite.

September 2017: Establishment of first inter-city secure quantum communications line, running 2,000 km from Beijing to Shanghai. It was used for the first quantum telephone call.

March 2020: Development of secure quantum key distribution protocol for ground-to-satellite transmissions. Performance beats world record.

December 2020: Achievement of quantum supremacy using light (i.e., a quantum computer based on the integrated photonics methodology).

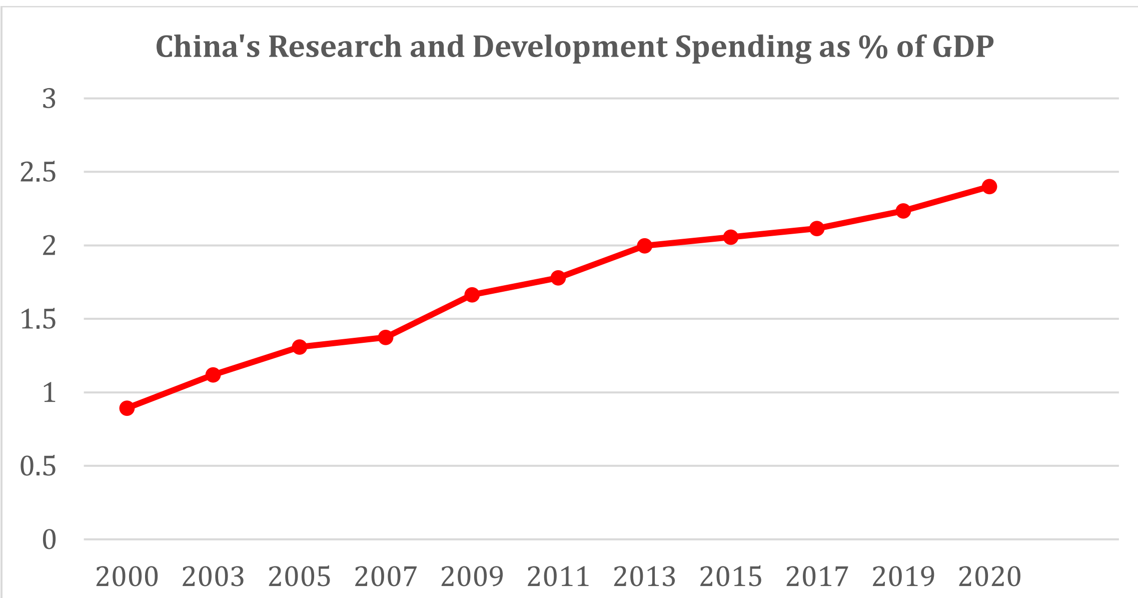
[28] The totals as of September 2020 were: PsiQuantum – US$500 million; D-Wave – US$300 million; Rigetti – US$200 million; Cambridge Quantum Computing – US$91 million; and IonQ – US$82 million. The author calculated these numbers with partial reference to "When Will We See Quantum IPOs?"Quantum Zeitgeist, September 25, 2020, https://quantumzeitgeist.com/when-will-we-see-quantum-ipos/.
[29] Sara Castellanos, "Xanadu Lands $100 Million as Investments Pour into Quantum Computing," *Wall Street Journal*, May 25, 2021, https://www.wsj.com/articles/xanadu-lands-100-million-as-investments-pour-into-quantum-computing-11621944002.

China

Over the past decade, China has worked diligently to modernize its national research and development system and to increase its efforts in key strategic areas. Quantum technologies have steadily featured more prominently in this push. In its 13th Five-Year Plan, which was released in 2016, China announced that it would pursue a "megaproject" on quantum communications and computing.[30] As part of these efforts, in 2017, China announced the investment of $10 billion to build a national laboratory for quantum information sciences in Hefei, Anhui Province.[31] (Hefei is home to the University of Science and Technology of China). China also has important national quantum research centres in Shanghai and Jinan. In addition, Chinese tech giants Tencent, Alibaba and Baidu have their own quantum research laboratories.[32] Part of China's investments include establishing the backbone of a quantum communications network that connects secure nodes in Beijing and Shanghai. This is designed for high-priority, sensitive communications.

Chart 2

Steadily Upward: China's Spending on Research and Development: 2000-2020[33]



Source: OECD

Getting accurate numbers about what China accurately spends on quantum is a challenge. Arthur Herman, a quantum expert at the Hudson Institute, stated in November 2019 that China spends

[30] Elsa Kania, "China's Quantum Future," Center for a New American Security, September 27, 2018, https://www.cnas.org/publications/commentary/chinas-quantum-future.
[31] Jeffrey Lin and P. W. Singer, "China is Opening a New Quantum Research Supercenter," *Popular Science*, October 10, 2017, https://www.popsci.com/chinas-launches-new-quantum-research-supercenter/.
[32] Inria, "Who Are the Main Players in the World of Quantum Computing?" December 16, 2020, https://www.inria.fr/en/quantum-computing-main-players.
[33] "Gross Domestic Spending on R&D," OECD, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm.

at least US$2.5 billion per year on quantum research.[34] Spending projections issued by the National Bureau of Statistics, on which the OECD numbers are based, also presumably exclude military research and development spending. These numbers show that China spent the equivalent of US$378 billion on research and development in 2020 – up 10.3 per cent from the year before.[35] The specific numbers for quantum are not disaggregated. What we do know is that quantum is a growing priority within a Chinese research and development system whose budget is growing in absolute and relative terms every year. If one had to make an educated guess about annual public-sector spending on quantum, somewhere in the range of US$10 billion per year seems probable at this point.

In March 2021, the Chinese government released its 14th Five-Year Plan. The plan lists those areas that are considered essential to "national security and overall development." It will:

> focus our aim on artificial intelligence (AI), quantum information, integrated circuits, life and health, brain science, bioengineered breeding, aerospace technology, deep earth and deep sea, and other cutting-edge fields, and carry out a set of major forward-looking and strategic national S&T projects.[36]

The 14th Five Year Plan commits to growing R&D spending by seven per cent per annum through 2025. Importantly, there is a significant emphasis on self-sufficiency in science and technology. Reducing dependence on the United States is a particular priority.[37] Now that China has built its infrastructure, one should expect it to roll out a steady stream of quantum innovations over the next decade.

United Kingdom

The United Kingdom has moved aggressively to pursue a leadership position in the global quantum revolution. In March 2015, the U.K. released its National Strategy for Quantum Technologies.[38] At the forefront of its recommendations was to "invest in a 10-year programme of support for academia, industry and other partners to jointly accelerate the growth of the UK quantum technologies ecosystem."

During the first phase, which ran from 2015 to 2020, the U.K. invested over £385 million across several government agencies. During the second phase, which runs through 2023, the U.K.

---

[34] Arthur Herman, "The Quantum Computing Threat to American Security," *Wall Street Journal*, November 10, 2019, https://www.wsj.com/articles/the-quantum-computing-threat-to-american-security-11573411715.

[35] Sam Shead, "China's Spending on Research and Development Hits a Record $378 Billion," CNBC, March 1, 2021, https://www.cnbc.com/2021/03/01/chinas-spending-on-rd-hits-a-record-378-billion.html#:~:text=China's%20spending%20on%20research%20and%20development%20climbed%2010.3%25%20to%202.44,nation's%20National%20Bureau%20of%20Statistics.&text=It's%20a%20new%20record%20for,a%2012.5%25%20rise%20in%202019.

[36] Xinhua News Agency, "Proposal of the Central Committee of the Chinese Communist Party on Drawing Up the 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2030," 7, Center for Security and Emerging Technology, Georgetown University, https://cset.georgetown.edu/wp-content/uploads/t0237_5th_Plenum_Proposal_EN-1.pdf.

[37] Smriti Mallapaty, "China's Five-year Plan Focuses on Scientific Self-reliance," *Nature*, March 11, 2021, https://www.nature.com/articles/d41586-021-00638-3.

[38] Innovate UK, "National Strategy for Quantum Technologies," Government of the United Kingdom, March 2015, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/414788/Strategy_QuantumTechnology_T15-080_final.pdf.

government will spend a minimum of £250 million. With additional government and industry investments, commitments are now well over £1 billion.[39] The U.K. has established four leading hubs built around consortiums of universities. The lead institutions are Birmingham (focus: sensors and timing); Glasgow (imaging); Oxford (computing and simulation); and York (quantum communications). It has also established a National Quantum Computing Centre, located in Oxfordshire.

The U.K. has a strong quantum ecosystem and is seen as a prime location for Western quantum firms to establish themselves. Cambridge Quantum Computing, for example, is one of the largest pure-play quantum companies in the world. In December 2020, it completed a US$45 million capital raise. It had previously raised US$46 million. Cambridge has four main business lines: (1) a hardware-agnostic software stack and (what appears to be) a best-in-class compiler called t|ket>; (2) a quantum chemistry tool called EUMEN, which is used in the design of pharmaceuticals and precision chemicals; (3) quantum machine learning; and (4) quantum cyber-security, including an encryption tool called Ironbridge.

The U.K.'s emphasis on quantum has even extended to the realm of international strategy. Its post-Brexit integrated review of security, defence, development and foreign policy put science and technology at the forefront and included a case study in the future role of quantum technologies across all of these areas.[40]

Europe

The European Union (EU) and its member states are investing significant funds in research and development related to quantum technologies. In October 2018, the EU launched the Quantum Technologies Flagship. Its initial budget of €152 million through September 2021 will grow to at least €1 billion by 2028. The Flagship has a total of 24 projects across four core areas of application:

- Quantum computing
- Quantum simulation
- Quantum communication
- Quantum metrology and sensing[41]

European member states are also stepping up with significant investments. Germany has been the only country led by someone who is truly a quantum expert. Outgoing Chancellor Angela Merkel obtained her doctorate in quantum chemistry in 1986 and worked as a practising scientist

[39] Peter Knight and Ian Walmsley, "UK National Quantum Technology Programme," *Quantum Science and Technology*, 2019, IOP Ebook, https://iopscience.iop.org/article/10.1088/2058-9565/ab4346/pdf.
[40] Cabinet Office, "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy," Government of the United Kingdom, March 16, 2021,https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.
[41] European Commission, "Quantum Technologies Flagship, " https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship.

until the fall of the Berlin Wall in 1989.[42] In June 2020, Merkel announced that her country would invest €2 billion in quantum technologies. She put down her marker by stating: "[I]t is our goal that Germany should be at the top of the world in terms of economics and technology in key areas of quantum technology, especially quantum computing, quantum communication, quantum sensor technology and quantum cryptography."[43]

She specifically noted that Germany will commission the construction of two quantum computers. Total budgeted spending through 2025 is estimated as the equivalent of US$3.1 billion.

In addition, France is making significant investments. In January 2021, President Emmanuel Macron announced that France would invest €1.8 billion (US$2.1 billion) with the goal of making France one of the top three nations in the world in quantum (along with the United States and China).[44] Of these investments, €1.05 billion will come from the French government, €200 million from the European Union and €550 million from the private sector. Of this, €800 million will go to quantum computing, €320 million to quantum communications and €250 million to sensors.

France began developing its quantum strategy in April 2019 when the government convened a panel of public- and private-sector leaders to study the challenge. Their report « Quantique: le virage technologique que la France ne ratera pas » ("Quantum: The Technological Shift that France Will Not Miss Out On") was released in January 2020.[45] The document provides the key policy foundations for the aforementioned investments.

The core challenge that Europe faces in the quantum revolution is that its model is good at funding core research and less good at commercializing resulting technologies.[46] The EU and its various member states are trying various formulations to overcome these difficulties and ensure that quantum is different. To that end, leaders in the bloc have pulled together an EU-wide European Quantum Industry Consortium as a way of encouraging various players to collaborate.[47]

[42] Business Insider, "Angela Merkel's Incredible Rise from Quantum Chemist to the World's Most Powerful Woman," July 26, 2021, https://www.businessinsider.in/politics/angela-merkels-incredible-rise-from-quantum-chemist-to-the-worlds-most-powerful-woman/slidelist/49302704.cms.

[43] Matt Swayne, "Qubit Alles: Germany to Invest 2 Billion Euros in Quantum Technology, Build Two Quantum Computers," The Quantum Daily, June 15, 2020, https://www.thequantumdaily.com/2020/06/15/qubit-alles-germany-invest-2-billion-euros-in-quantum-technology-build-two-quantum-computers/.

[44] Staff, Le Monde/Agence France-Presse, « Emmanuel Macron veut mettre la France dans le trio de tête mondial des technologies quantiques, » *Le Monde*, January 21, 2021. https://www.lemonde.fr/politique/article/2021/01/21/emmanuel-macron-presente-un-plan-quantique-de-1-8-milliard-d-euros-sur-cinq-ans_6067037_823448.html.

[45] Neil Abroug, Thierry David, Matthieu Ratieville, and Jean Vannimenus, « Quantique: le virage technologique que la France ne ratera pas » January 2020, https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf.

[46] This is a good example of their strategies in action. IQM Finland Oy, "New EU Consortium Shaping the Future of Quantum Computing," Cision PR Newswire, February 12, 2021, https://www.prnewswire.com/news-releases/new-eu-consortium-shaping-the-future-of-quantum-computing-301227670.html.

[47] European Quantum Industry Consortium, https://qt.eu/quic-status/.

Japan

Japan is regarded as a bit of a dark horse in the quantum race, although given its superb tradition of technological breakthroughs, it seems destined to be a top-tier nation in this domain. Japan has been working on quantum topics since the mid-1980s.[48]

In its 2020 budget, the government made a flagship investment of ¥30 billion (US$260 million) over five years for quantum. This is in addition to a range of other projects on which the Japanese government, private sector and universities are closely collaborating. For example, building a "fault-tolerant universal (quantum) computer" is one of the seven "high-risk, high-reward" transformational projects under the Cabinet Office's "Moonshot Research and Development Program."[49] The estimated budget is ¥14.5 billion (US$128 million) through 2050.[50] In 2020, major Japanese firms from Toshiba and Toyota to Mitsubishi and Hitachi joined forces with IBM Japan, Keio University and the University of Tokyo to form the Quantum Innovation Initiative Consortium. It aims to develop useful applications for quantum computing in the near future.[51]

IBM's inclusion in the Japanese consortium is part of an interesting shift. Japan is more willing than in the past to partner with non-Japanese entities in the development of core technologies. To that end, the United States and Japan signed the Tokyo Statement on Quantum Collaboration in December 2019.[52] It specifically commits the two countries to "pursue cooperation and the mutual respect it confers, and to promote QIST (quantum information science and technology) including but not limited to quantum computing, quantum networking, and quantum sensing, which underpins the development of society and industry." This will undoubtedly evolve into a coherent plan.

United States

In discussing quantum in the United States, there are two eras: before December 21, 2018, and after. On that day, the *National Quantum Initiative Act* was signed into law by then-president Donald Trump. The NQI has given focus and resources to U.S. quantum efforts. Its stated objective is to advance basic and applied research in quantum information science (QIS) by civilian agencies, institutions and companies. There are parallel efforts underway in the defence and intelligence communities that have separate budget allocations. Of course, civilian applications can often have dual applicability to national defence.

The NQI defines quantum information science as "the use of the laws of quantum physics for the storage, transmission, manipulation, computing, or measurement of information." This covers activities ranging from sensing and metrology to computing and simulation.[53] Computing has

[48] Y. Yamamoto, et al., "Quantum Information Science and Technology in Japan," *Quantum Science and Technology*, February 22, 2019, https://iopscience.iop.org/article/10.1088/2058-9565/ab0077/pdf.
[49] Cabinet Office of Japan, Moonshot Research and Development Program, https://www8.cao.go.jp/cstp/english/moonshot/top.html.
[50] Ibid. The projected financial investment is 1/7 of the total Moonshot budget.
[51] Akira Oikawa, "Japan Group to Bring Quantum Computers to the Workplace," *Nikkei Asia*, July 31, 2020, https://asia.nikkei.com/Business/Technology/Japan-group-to-bring-quantum-computers-to-the-workplace.
[52] Tokyo Statement on Quantum Collaboration, https://www.state.gov/tokyo-statement-on-quantum-cooperation/.
[53] Staff, "Quantum Information Science: Applications, Global Research and Development, and Policy Considerations," Congressional Research Service, Government of the United States, December 14, 2018, https://fas.org/sgp/crs/misc/R45409.pdf.

emerged as the centrepiece, followed by communications (i.e., the National Quantum Internet project).

Watching quantum developments in China, the Trump administration and members of Congress became convinced of the need for the U.S. to make a major push in this area. A series of workshops, hearings and discussions were held. In September 2018, the Quantum Information Science Sub-Committee of the Office of Science and Technology Policy (OSTP) issued a National Strategic Overview,[54] whose content looked a lot like that of the NQI.

In terms of budget, the NQI allocates $1.275 billion for FY2019-2023 to "secure American dominance over the increasingly competitive fields related to quantum technology and theory." A subsequent amount will be determined for the FY2024-2028 period. Since its passage, first the Trump administration and now the Biden administration have pursued major increases.

Table 3

The *National Quantum Initiatives Act* (NQI): A Summary[55]

NQI Areas of Focus
(1) Supporting research, development, demonstration and application of quantum information science and technology: (A) To expand the number of researchers, educators and students with training in quantum information science and technology; (B) To promote the development and inclusion of multidisciplinary curriculum and research opportunities for quantum information science at the undergraduate, graduate and postdoctoral levels; (C) To address basic research knowledge gaps; (D) To promote the development of facilities and centres available for quantum research, testing and education; and (E) To stimulate research and promote rapid development of quantum technologies; (2) Improving the interagency planning and co-ordination on quantum;

[54] U.S. National Science and Technology Council, "National Strategic Overview for Quantum Information Science," September 2018, https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf.
[55] *National Quantum Initiative Act*, https://www.congress.gov/bill/115th-congress/house-bill/6227.

(3) Maximizing the effectiveness of the federal government's quantum information science and technology research, development and demonstration programs;

(4) Promoting collaboration among the government, national laboratories, industry and universities; and

(5) Promoting the development of international standards for quantum information science and technology security:

(A) To facilitate innovation and private-sector commercialization; and

(B) To meet economic and national security goals.

The Department of Energy (DOE), which runs most of the U.S. system of national laboratories, got the biggest share of the NQI budget. On August 26, 2020, DOE announced that US$625 million would be allocated to five national laboratories to establish five new quantum information science centres. These funds will be allocated at a rate of US$25 million per year per centre for five years. The recipients are Argonne, Brookhaven, Fermilab, Oak Ridge and Lawrence Berkeley national laboratories.[56] The centres will focus on a range of key QIS research topics including quantum networking, sensing, computing and materials manufacturing. Importantly, the private sector matched these funds with US$340 million. Partners include IBM, Microsoft, Intel, ColdQuanta and Rigetti. IBM, for example, will be a partner at three of the new QIS centres.[57]

Canadians are also involved in a number of U.S. initiatives. At least two of the five QIS centres already publicly note having Canadian advisors or consortium members. The Quantum Systems Accelerator program at Lawrence Berkeley National Laboratory lists the Université de Sherbrooke among the 15 members of its consortium. It is the only international partner. At the Quantum Science Center at Oak Ridge National Laboratory, two of the 11 scientific advisors are from Canadian institutions: David Cory from the University of Waterloo and Marcel Franz from the University of British Columbia. However, it appears that no Canadian institutions are members. The QIS centres made these arrangements directly with the Canadian researchers without any known facilitation by the Canadian government.

Another major investment under the NQI was the allocation of US$75 million over five years from the National Science Foundation (NSF) to set up "Quantum Leap Challenge Institutes." These

[56] U.S. Department of Energy, "White House Office of Technology Policy, National Science Foundation and Department of Energy Announce Over $1 Billion in Awards for Artificial Intelligence and Quantum Information Science Research Institutes," Government of the United States, August 26, 2020, https://www.energy.gov/articles/white-house-office-technology-policy-national-science-foundation-and-department-energy.

[57] IBM's specific contribution, for example, is described in: "Five Things to Know about the New National Quantum Centers," IBM, August 26, 2020, https://newsroom.ibm.com/2020-08-26-Five-Things-to-Know-About-the-New-National-Quantum-Centers.

institutes are large-scale interdisciplinary research projects that aim to advance the frontiers of quantum information science and engineering. Research will span the focus areas of quantum computation, quantum communication, quantum simulation and/or quantum sensing.[58] In July 2020, these were awarded to the University of Colorado; University of Illinois – Urbana-Champaign and University of California – Berkeley.

As the DOE and NSF programs demonstrate, collaboration among government, academia and the private sector is seen as the way forward for making progress on quantum computing. In this spirit, a number of companies have taken to establishing quantum research centres on select university campuses in the United States and globally. For example, in December 2019, AWS announced a partnership with Caltech to establish the AWS Center for Quantum Computing on the university's campus in Pasadena, California. The centre aims to develop more powerful quantum hardware and software and identify new applications for quantum technologies. The centre has a research staff and hosts "Amazon scholars" from around the world. Its initial work is on quantum algorithms and hardware. By placing centres like this on campuses with a strong track record of innovation, companies seek to seed and commercialize the next breakthroughs in the quantum realm.

Table 4

Who is Doing What at the National QIS Centres?[59]

Project	**Lead Institution**	**Focus Area**	**Notable Partners**
Q-NEXT	Argonne National Laboratory (Illinois)	Establish efficient quantum networks for information processing with scalable hardware.	IBM, Microsoft, Intel, Boeing, ColdQuanta, University of Chicago, University of Illinois, Caltech.
Co-design Center for Quantum Advantage (C2QA)	Brookhaven National Laboratory (New York)	Deliver 10x improvement in software optimization, materials and device properties, and quantum error correction to provide a 1,000x improvement in computation.	IBM, MIT, Yale, Stony Brook University, Princeton, Pacific Northwest National Lab.

[58] Quantum Leap Challenge Institutes, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505634.
[59] Please see U.S. Department of Energy, National QIS Research Centers, https://science.osti.gov/Initiatives/QIS/QIS-Centers.

Superconducting Quantum Materials and Systems Center	Fermilab (Illinois)	Make revolutionary advances in quantum computing and sensing, including the building and deployment of a beyond-the-state-of-the-art quantum computer.	Rigetti Computing, Northwestern University, Ames Research Center (NASA), Ames Laboratory.
Quantum Systems Accelerator	Lawrence Berkeley National Laboratory (California)	Identify the most impactful scientific applications that stand to benefit from quantum computing and engineer the hardware and software systems to run these applications.	Sandia National Lab, University of Colorado at Boulder, MIT Lincoln Laboratory, Caltech, UC Berkeley, Maryland, Université de Sherbrooke.
Quantum Science Center (QSC)	Oak Ridge National Lab (Tennessee)	Harness and control quantum coherence for new applications of QIS for sensing and scientific discovery.	Los Alamos National Lab, Berkeley, IBM, Microsoft, ColdQuanta, Fermilab, Harvard, University of Maryland.

Another focus coming out of the NQI is in the realm of quantum communications. The United States is committing to build out a national quantum internet within 10 years. The vision is to have the communications backbone – hardware, software and systems – fully developed and widely enough disseminated to allow the country to take full advantage of these breakthrough technologies.

On July 23, 2020, DOE and David Awschalom of the University of Chicago/Argonne National Lab (representing the research community) presented the technical roadmap for how this will be done.[60] It was substantially developed by 50 participants at a workshop that DOE hosted in February 2020.[61] The technical report found that mastery was required in three areas in order for a quantum internet to be successfully constructed:

[60] U.S. Department of Energy, "U.S. Department of Energy Unveils Blueprint for the Quantum Internet at 'Launch to the Future: Quantum Internet' Event," Government of the United States, July 23, 2020, https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet.

[61] Ibid., "From Long-distance Entanglement to Building a Nationwide Quantum Internet," February 5-6, 2020, https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt20FINAL_Nav_0.pdf.

1. Building and then integrating quantum networking devices;
2. Perpetuating and routing quantum information; and
3. Correcting errors/ensuring accuracy of information.

In terms of physical construction of a national quantum internet, the technical report established four key milestones:

1. Verify secure quantum protocols over existing fibre networks;
2. Send entangled information across campuses or cities;
3. Expand the networks between cities; and
4. Expand between states, using quantum repeaters to amplify signals.

As a preliminary step while the technical report was being developed, Argonne National Laboratory and the University of Chicago successfully sent entangled photons along a 52-mile quantum loop. Fermi National Accelerator Laboratory is now being added, making it a three-node, 80-mile testbed in the Chicago area.[62] Entangled information has tended to become corrupted after only 150 miles when sent on optical fibre. This testbed will be steadily expanded as technical challenges are overcome.

Canada has not been invited to participate in the U.S. national quantum internet project nor has it sought to join.

While U.S. efforts are yielding substantial innovation in quantum technologies, the rest of the world has begun to run much faster since the NQI's passage. Anxiety about China's quantum advances is particularly acute. The *National Defense Authorization Act* (NDAA), which passed Congress in January 2021, included significant quantum provisions. Among other things, it ordered each service branch to develop a list of technical problems and research questions potentially addressable by quantum computing and a path for working with research institutions and the private sector to resolve them. It also prominently featured quantum in the mandate of the high-level steering group on emerging threats. In addition, the NDAA ordered a "comprehensive assessment of the current and potential threats and risks posed by quantum computing technologies to critical national security systems." Finally, it committed to increase funding for "industries of the future" to US$10 billion per year by 2025.[63] While the NDAA did not offer a specific definition of these industries, during the Trump years it was assumed to mean artificial intelligence, quantum information science, 5G telecommunications, biotechnology and advanced manufacturing.[64]

[62] Ibid., "U.S. Department of Energy Unveils Blueprint …"
[63] U.S. House of Representatives, "William M. (Mac) Thornberry *National Defense Authorization Act* for Fiscal Year 2021," Government of the United States, December 3, 2020, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf.
[64] American Institute of Physics, "FY21 NDAA Enacted: Science and Technology Policy Highlights," March 9, 2021, https://www.aip.org/fyi/2021/fy21-ndaa-enacted-science-and-technology-policy-highlights.

Quantum in Canada

Unlike many countries, Canada enters the quantum revolution with an extraordinarily rich ecosystem of research centres, companies and capacities, built with patient and intelligent investments over many years. Canada is a true global leader in quantum and is well positioned to remain so, but as they say in investing, "past performance is no guarantee of future results." Before offering suggestions on what Canada should do in the short to medium term to extend its national quantum advantage, it is important to explain its capacities in some detail, beginning with some of Canada's major quantum centres.

Waterloo

Waterloo, Ontario has been famous for technology since Research in Motion (now BlackBerry) grew into a global company. BlackBerry co-founder Mike Lazaridis envisioned a world-class research centre in Waterloo devoted to the study of theoretical physics, including quantum. He was the key driver behind the creation of the Perimeter Institute of Theoretical Physics, which he endowed with C$100 million. The federal and Ontario governments contributed a total of C$40 million to launch the institute in 2000. Both levels of government have continued to renew their support over the years.[65] In October 2020, Perimeter established the Clay Riddell Centre for Quantum Matter with an endowment of C$25 million.[66] Perimeter remains a global leader in this space.

Lazaridis, however, was not content with endowing Perimeter alone. In 2002, he gave millions more to establish the Institute of Quantum Computing (IQC) at the University of Waterloo.[67] Lazaridis and university president David Johnston (later Governor General of Canada) teamed up to recruit Raymond Laflamme[68] as its executive director. Laflamme was born in Quebec City, had Stephen Hawking as his PhD supervisor at Cambridge and was an Oppenheimer Fellow at Los Alamos National Lab. Since its founding, IQC has built a world-class reputation and has achieved several breakthroughs in the quantum computing field.

As with Perimeter, the federal and provincial governments have provided significant ongoing support to IQC as well as stand-alone investments. The biggest of these was C$76.2 million in 2016 for the "Transformative Quantum Technologies" initiative under the Canada First Research Excellence Fund (CFREF).[69] With such strong support, Waterloo has been able to pursue some of the biggest questions in quantum and has established a reputation as one of the leading global centres in the field. CFREF is an example of big science – an ethos of investing heavily in world-class centres of excellence rather than sprinkling funds across several smaller projects.

---

[65] Perimeter Institute of Theoretical Physics, "History," https://perimeterinstitute.ca/history.
[66] Ibid., "Perimeter Institute launches Clay Riddell Centre for Quantum Matter," Newswise, October 15, 2020, https://www.newswise.com/articles/perimeter-institute-launches-clay-riddell-centre-for-quantum-matter.
[67] Institute for Quantum Computing, https://uwaterloo.ca/institute-for-quantum-computing/.
[68] Ibid., "Raymond Laflamme," https://uwaterloo.ca/institute-for-quantum-computing/people-profiles/raymond-laflamme.
[69] Canada First Research Excellence Fund, "Government of Canada Invests $900 Million to Transform University Research," Sept. 6, 2016, https://www.cfref-apogee.gc.ca/news_room-salle_de_presse/press_releases-communiques/2016/University_of_Waterloo-eng.aspx.

A number of important quantum companies have emerged from the Waterloo ecosystem. They include:

- Quantum Benchmark: Led by a notable team of quantum researchers, the company provides software that enables error characterization, error mitigation, error correction and performance validation for quantum computing hardware;[70] and

- QEYnet: Founded in 2016, this innovative company seeks to provide a global, low-cost, micro satellite-enabled quantum key distribution network. As Project Jinan, among other experiments, has shown, satellites will be an integral part of any quantum internet.[71]

Vancouver

In 1999, a group out of the University of British Columbia (UBC) founded a breakthrough quantum computing company. D-Wave Systems[72] is arguably the most commercially successful quantum company. In the early years, it worked with universities and research institutions across the world, including UBC, Université de Sherbrooke and the University of Toronto. In 2008, D-Wave introduced and sold a 28-qubit computer. In 2011, it rolled out D-Wave One, which had a 128-qubit chip set and was billed as the "world's first commercially available quantum computer." D-Wave has engaged with a variety of customers. Some U.S. government agencies have purchased D-Wave computers outright. Others, including leading global companies, have partnered with D-Wave to use its technology for specific projects. Regardless of the model, D-Wave has fundamentally contributed to making quantum computing more widely available.

D-Wave computers are built on the quantum annealing methodology, which is ideally designed to solve optimization problems. In other words, it defines the best or most efficient way to do something across a vast, but ultimately finite array of possibilities.[73] On September 29, 2020, D-Wave launched its fifth-generation quantum computer, which was dubbed "Leap." Because D-Wave was first to market and uses a different technology than most other quantum computers, critics often alleged that it would not scale. Gate systems feel more like traditional computers in that they excel in addressing many types of problems.[74] D-Wave's Leap system has over 5,000 qubits and 15-qubit connectivity. That is up from 2,000 qubits and six-way connectivity in the previous generation. In short, it is scalable. In addition to Leap, D-Wave has launched a hybrid problem solver that lets customers integrate traditional and quantum computers. Specifically, it breaks a computing task into components, some of which are solved using a quantum computer and some using a traditional computer, all delivered through a cloud-based interface.[75]

[70] Quantum Benchmark, https://quantumbenchmark.com/.
[71] "The Approaching Quantum Threat," QEYnet, https://www.qeynet.com/.
[72] D-Wave Systems, https://www.dwavesys.com/.
[73] Ibid., "What is Quantum Annealing?" https://docs.dwavesys.com/docs/latest/c_gs_2.html.
[74] Una Wang, "What is Quantum Annealing and How Does it Differ from Gate Based Quantum Computers?" Quantum Zeitgeist, October 24, 2020, https://quantumzeitgeist.com/what-is-quantum-annealing-and-how-does-it-differ-from-gate-based-quantum-computers/.
[75] Jeremy Kahn, "D-Wave Unveils Its Most Powerful Quantum Computer to Date," *Fortune*, September 29, 2020, https://fortune.com/2020/09/29/d-wave-5000-qubit-quantum-computer/.

In addition to D-Wave, Vancouver founded 1Qbit[76] in 2012. It focuses on making the enabling elements of the quantum revolution work, both in optimizing quantum computing and applying it in interesting areas through a widely accessible, hardware-agnostic software platform. Its 1Qloud platform is a computational bridge that enables operations researchers, data scientists and developers to harness the power of advanced computing resources and novel algorithms without the need to learn the intricacies of each individual hardware platform or to manage complex and expensive computing infrastructure. One of its most interesting tools is a quantum-enabled molecular simulation toolkit, or QEMIST. It can be used to accurately predict a molecule's structure, which is very useful in new drug development and the design of specialized materials. It also has a quantum-enabled algorithmic trading platform that it uses to manage risk on futures contracts. It administers this jointly with Chicago's CME. 1Qbit has a very close relationship with Microsoft. The World Economic Forum has named it a global technology pioneer.

An excellent local academic infrastructure supports D-Wave, 1Qbit and others. UBC has a quantum research excellence cluster that pulls together faculty from physics, chemistry and engineering.[77] In addition, UBC hosts the Stewart Blusson Quantum Matter Institute (SBQMI).[78] With significant support from CFREF and partnerships with the University of Tokyo and the Max Planck Institute for Solid State Research in Stuttgart, Germany, SBQMI has launched a new joint PhD program in quantum materials.

Simon Fraser University (SFU) is also moving aggressively to carve out its lanes in the quantum race. SFU has the Silicon Quantum Technology Lab in its Department of Physics, which focuses on building quantum technologies using silicon.[79] In addition, in 2019, the B.C. government supported the establishment of the Quantum Algorithms Institute at Simon Fraser.[80] It has many leading global industry partners, including AWS, IBM and Microsoft, as well as leading B.C. quantum companies and universities.

Toronto

In recent years, Toronto has developed an interesting and diverse quantum ecosystem. It is home to Xanadu, which seems to be on everyone's list of companies to watch. Like PsiQuantum in Silicon Valley and a leading university consortium in China, Xanadu is building a quantum computer that applies an integrated photonics methodology. Unlike, for example, the Google and IBM systems, which use superconducting circuits, photonic-based quantum computers can function at room temperature and do not require ultra-cold fridges to function.

On September 2, 2020, Xanadu became the first company to offer cloud access to gate-based photonic quantum computers. Customers will be able to use either an eight-qubit or a 12-qubit machine with a 24-qubit processor promised shortly. Robert Niffenegger, of the MIT Lincoln

[76] 1Qbit, https://1qbit.com/.
[77] University of British Columbia, "Quantum Computing," https://quantumcomputing.ubc.ca/.
[78] Ibid.," https://qmi.ubc.ca/.
[79] Simon Fraser University, "Silicon Quantum Technology Lab," https://www.sfu.ca/physics/siliconquantum/.
[80] Ibid., Quantum Algorithms Institute, https://quantumalgorithms.ca/.

Laboratory, called Xanadu's ability to allow users to access its photonic circuits via the cloud, "very impressive" and "a first."[81]

Xanadu is also known for two open-source technology-agnostic tools: PennyLane, an open-source software library for quantum machine learning, quantum computing and quantum chemistry, and Strawberry Fields, its cross-platform Python language library for simulating and executing programs on quantum photonic hardware.[82]

Xanadu has the backing of some of Canada's most important venture capital funds, including OMERS, Georgian and BDC. After its successful cloud launch in September 2020, the company set out to raise US$100 million to grow its quantum computer from 40 qubits to one million qubits by 2026.[83] Xanadu closed its successful US$100 million Series B Round in May 2021. Silicon Valley's Bessemer Venture Partners took the lead role in its just-completed funding round. Xanadu is already generating significant revenue through its cloud services.[84]

The University of Toronto, a world-class academic research institution in this field, is a key anchor for the city's quantum ecosystem. The Centre for Quantum Information and Quantum Control (CQIUC) is a collaboration across six departments. It has a big faculty and numerous postdoctoral fellows.

In 2018, Alán Aspuru-Guzik was awarded a Canada 150 Research Chair to work on quantum issues at the University of Toronto. In Budget 2017, C$117.5 million was allocated to enhance Canada's reputation in science and innovation by bringing top-tier internationally based scholars and researchers to Canada. The funds are co-administered by the granting councils, including the Natural Sciences and Engineering Research Council (NSERC). Aspuru-Guzik is receiving C$1 million per year for seven years under the program as the Research Chair for Theoretical and Quantum Chemistry.[85]

After finishing his PhD at UC Berkeley, Aspuru-Guzik moved to Boston where he taught at Harvard University. Gradually, he began to put together Zapata Computing, which was founded as a software company for quantum computers. Orquestra, their main product, is described as "the first and only end-to-end, workflow-based toolset for quantum computing." It is all about collaboration at scale. The company notes that Orquestra is purpose-built for quantum machine learning, optimization and simulation problems across industries.

[81] Paul Smith-Goodson, "Xanadu Brings Photonic Quantum Computing to the Cloud," *Forbes*, September 9, 2020, https://www.forbes.com/sites/moorinsights/2020/09/09/xanadu-brings-photonic-quantum-computing-to-the-cloud/#1a79fe2f64e6.
[82] Emil Protalinski, "Xanadu Launches Quantum Cloud Platform, Plans to Double Qubits Every 6 Months," VentureBeat, September 2, 2020, https://venturebeat.com/2020/09/02/xanadu-photonics-quantum-cloud-platform/.
[83] Sean Silcoff, "Toronto Quantum Computer Startup Xanadu Eyes $100-million Funding After Launching Online Service," *Globe and Mail*, September 2, 2020, https://www.theglobeandmail.com/business/article-toronto-quantum-computer-startup-xanadu-eyes-100-million-funding/.
[84] Sara Castellanos, "Xanadu Lands $100 Million as Investments Pour into Quantum Computing," *Wall Street Journal*, May 25, 2021, https://www.wsj.com/articles/xanadu-lands-100-million-as-investments-pour-into-quantum-computing-11621944002.
[85] Government of Canada, "Canada 150 Research Chairs," https://www.canada150.chairs-chaires.gc.ca/chairholders-titulaires/index-eng.aspx.

Since Aspuru-Guzik's arrival in Canada, Zapata has prioritized expansion in Toronto. As part of its Canadianization, Zapata was a founding member of Quantum Industry Canada,[86] the industry body that brings together most of the players in the Canadian quantum sector.

Toronto is also home to Creative Destruction Lab (CDL).[87] Housed at the Rotman School of Management at the University of Toronto, CDL provides an array of mentorship, training and support to scalable seed-stage science and technology-based companies. Quantum is one of 15 streams. A variety of notable quantum start-up companies have benefited from CDL support.

Sherbrooke

In 2016, L'institut quantique (IQ) at Université de Sherbrooke[88] was founded through a C$74 million investment by CFREF. Sherbrooke was a natural choice given its decades of basic research in the quantum domain. L'institut works at the intersection of quantum materials, quantum information and quantum engineering. It has produced a number of start-ups and techniques that are being commercialized.[89]

A huge step forward for Sherbrooke's global visibility as a quantum hub came in June 2020. IBM Q, the quantum division of IBM, reached an agreement with L'institut quantique (IQ) to become an IBM Q hub. This is the first such hub in Canada and one of 14 in the world. The Quebec government provided C$4.5 million to support its work.[90]

Alberta

Alberta has significant quantum resources at the universities of Calgary, Alberta and Lethbridge. As part of its economic diversification efforts, the province has worked with the universities to set up Quantum Alberta.[91] It focuses on enabling both research and commercialization.

The University of Calgary's Institute for Quantum Science and Technology[92] is getting the most notice among the participating institutions. One important area of focus is teleportation. The concept is roughly the same idea as in Star Trek, except they are beaming up entangled photons of light rather than physical objects. In 2016, Calgary researchers sent a particle of light six kilometres through the city's fibre network.[93] In December 2020, Calgary scientists teamed up with peers at Caltech, FermiLab, AT&T, Harvard and the Jet Propulsion Laboratory to transmit light particles 44 kilometres via quantum teleportation.[94] Teleportation is a key technique for

[86] Quantum Industry Canada, https://www.quantumindustrycanada.ca/.
[87] Creative Destruction Lab, https://www.creativedestructionlab.com/.
[88] Université de Sherbrooke, « Institut Quantique » https://www.usherbrooke.ca/iq/en/.
[89] James Dargan, "Québec: Respected Centre for Canada's Quantum Innovation," The Quantum Daily, December 7, 2020, https://www.thequantumdaily.com/2020/12/07/quebec-respected-centre-for-canadas-quantum-innovation/.
[90] Université de Sherbrooke, "IBM Q Hub – L'Institut quantique at Université de Sherbrooke Joins IBM Q Network, " Cision Newswire, June 1, 2020, https://www.newswire.ca/news-releases/ibm-q-hub-l-institut-quantique-at-universite-de-sherbrooke-joins-ibm-q-network-866508171.html.
[91] Quantum Alberta, http://quantumalberta.ca/.
[92] Institute for Quantum Science and Technology, University of Calgary, https://www.iqst.ca/.
[93] Drew Scherban, "Beam Me Up Scotty! Researchers Teleport Particle of Light Six Kilometres," *UCalgary News*, August 20, 2016, https://ucalgary.ca/news/beam-me-scotty-researchers-teleport-particle-light-six-kilometres.
[94] Vincent Bonnay, « Des scientifiques réalisent une téléportation quantique sur 44 kilomètres, » RadioCanada, January 8, 2021, https://ici.radio-canada.ca/nouvelle/1761666/teleportation-internet-quantique-calgary-recherches.

making a quantum internet work at scale.[95] Others are taking notice. In October 2020, the Alberta government invested C$11.8 million in the Quantum Institute's work.[96]

Public Policy and Strategy

Canada's diverse quantum ecosystem did not evolve by accident. A combination of visionary leaders in the university and private sectors coupled with sound public policy and generous funding have positioned Canada to significantly benefit as quantum technologies mature and become commercially valuable.

In a 2019 article, "Quantum Canada," by Ben Sussman et al., the authors note that Canada's investments in this space averaged over C$100 million per year in the previous decade.[97] Policy-makers saw the quantum revolution coming and invested accordingly. Investments began to slowly increase after Gilles Brassard's BB84 breakthrough. In the 2000s, after D-Wave's founding, Canada took investments to a different level. The authors note, for example, that NSERC invested C$267 million in quantum between 2006 and 2015. The Canadian Foundation for Innovation, the Canadian Institute for Advanced Research and CFREF have also all invested heavily in making Canada's rich quantum ecosystem a reality. In addition to funding universities, government institutions, from the NRC to the Canadian Space Agency to the Communications Security Establishment, have received government support for substantial quantum projects. Overall, Canada ranks first in the G7 in per capita spending on quantum.[98]

Having established its strong position, there has been discussion in recent years about the development of a formal Canadian quantum strategy. In 2017, the National Research Council (NRC)commissioned a survey of key players in the quantum ecosystem about where they wanted things to go.[99] Since at least 2018, Canada has received strong overtures of co-operation from the U.S. and even stronger requests to collaborate with the U.K. on quantum, but these were not immediately actioned. A domestic strategy, including clear guidance on "machinery of government" questions (i.e., who has the lead authority), would have to be worked through before a bilateral agenda could be defined.

Even while Canada worked through its processes, the federal government continued to step forward and support the nation's burgeoning quantum economy. In March 2021, the government of Canada, through its Strategic Innovation Fund, invested C$40 million toward a C$120 million project of market leader D-Wave. According to the release:

---

[95] Maria Korolov. "Quantum Teleportation Makes Progress, But Toward What?" Data Center Knowledge, February 2, 2021, https://www.datacenterknowledge.com/networks/quantum-teleportation-makes-progress-toward-what.

[96] Sammy Hudes, "Province Gives $11.8M to U of C for Quantum Research, Other Projects," *Calgary Herald*, October 23, 2020, https://calgaryherald.com/news/local-news/diversifying-our-economy-has-never-been-more-important-province-gives-11-8m-to-u-of-c-for-quantum-research-other-projects.

[97] B. Sussman, et al., **"**Quantum Canada,**"** *Quantum Science and Technology*, February 22, 2019, https://iopscience.iop.org/article/10.1088/2058-9565/ab029d.

[98] Ibid.

[99] Canadian Institute for Advanced Research, "Quantum Canada Survey," March 2017, https://nrc.canada.ca/sites/default/files/2019-03/Quantum_Canada_Report_e.pdf.

> The investment will help D-Wave further the advantage of quantum technology over classical computers by enhancing the processing capabilities and computing power of its current systems. To reach this objective, the company will develop a new and more powerful quantum processor ...[100]

As part of the investment, D-Wave commits to create and maintain up to 200 jobs and invest C$480 million in research and development.

The NRC also played a significant role in setting up Quantum Industry Canada (QIC) – Canada's quantum industry association. QIC had 24 members when it launched in October 2020.[101]

On April 19, 2021, a big part of the question of how Canada will approach the next phase of the quantum revolution was answered. As per the Department of Finance release:

> Budget 2021 proposes to provide $360 million over seven years, starting in 2021-22, to launch a National Quantum Strategy. The strategy will amplify Canada's significant strength in quantum research; grow our quantum-ready technologies, companies, and talent; and solidify Canada's global leadership in this area. This funding will also establish a secretariat at the Department of Innovation, Science and Economic Development (ISED) to coordinate this work.[102]

In other words, Canada will spend over C$50 million per year to support the activities in its forthcoming quantum strategy. It also now will have the co-ordination infrastructure necessary to make decisions, including on whom to collaborate with internationally.

On July 16, 2021, the government of Canada advanced the development of the national quantum strategy through the release of an engagement paper and the launch of public consultations.[103]

Next Steps – Maintaining Leadership in the New Quantum Age

As noted, Canada enters the era of the applied quantum technology revolution extraordinarily well positioned. The key question is how best to extend these advantages. Some suggested pathways include:

National Economic Advantage

- *Use federal funding power to ensure collaboration among research centres*: One of the perennial challenges with Canadian federalism is the tendency toward regionalization.

[100] Innovation, Science and Economic Development Canada, "Government of Canada Contribution Strengthens Canada's Position as a Global Leader in Quantum Computing," Cision Newswire, March 11, 2021, https://www.newswire.ca/news-releases/government-of-canada-contribution-strengthens-canada-s-position-as-a-global-leader-in-quantum-computing-824210415.html.
[101] Quantum Industry Canada, https://www.quantumindustrycanada.ca/.
[102] Finance Canada, "Budget 2021: Building an Innovation Economy of the Future," Government of Canada, April 19, 2021, https://www.canada.ca/en/department-finance/news/2021/04/budget-2021-building-an-innovation-economy-of-the-future.html.
[103] Innovation, Science and Economic Development Canada, "Engagement Paper: Developing a National Quantum Strategy," Government of Canada, https://www.ic.gc.ca/eic/site/154.nsf/eng/00001.html.

When the B.C. government, for example, puts $17 million forward to create the Quantum Algorithms Institute at Simon Fraser, it wants in-province institutions (in this case, UBC and the University of Victoria) as the other academic partners. Canada has a rich array of quantum research hubs across the country. It is important to ensure that a key feature of major federal funding initiatives for quantum is a mandate to co-operate among centres cross-regionally. In 2016, when Canada announced substantial CFREF grants to Sherbrooke, UBC and Waterloo, the three institutions were required to work together on joint projects.[104] This type of mandated collaboration is very helpful to encouraging the development of synergies across the country. As the federal government moves to spend $50 million per year on quantum, ensuring ongoing cross-collaboration among different institutions across the country should be a priority. The ISED Secretariat could undoubtedly play a role in assessing where greater complementarities could be developed among institutions.

- *Concentrate resources on large projects with bigger teams*: In interviews with major quantum industry players in recent months, some common themes emerged. One theme related to the superb quality of quantum brainpower and basic research execution in Canada. Other themes related to the challenges of later stage development and commercialization. Success in quantum is likely to require, in many cases, a level of scale. A clear and specific recommendation was that Canada fund larger projects with bigger teams. This would provide greater scope for research progress and facilitate commercialization. These teams would ideally include experts from different quantum hubs across the country. By including students and post-docs in commercial projects, the quality of the training they will receive, including in how to manage a quantum venture, increases significantly.

- *Make bold bets in promising quantum companies*: Canada has some very good quantum companies. While D-Wave, 1Qbit and Xanadu are at the forefront in terms of funds raised, there are certainly others that are slightly smaller but poised to break through. As money pours into quantum across the world, including through investments by some of the world's largest IT players, the competition is dramatically increasing. The policy development process that led to the major quantum investment announced in the recent budget embraced the idea of bold investments in quantum companies poised to scale. The question is which companies and initiatives to prioritize. Canada should consider undertaking an analysis to determine, say, the top three to five most promising quantum companies which have secured investments of, say, less than C$10 million. It could do a separate analysis of promising micro-scale quantum companies that have secured, say, less than C$2 million. The federal government could match this by an assessment of specific proposed interventions.

[104] Emily Wight, "Joint CFREF Quantum Projects Announced," Stewart Blusson Quantum Matter Institute, University of British Columbia, March 5, 2019, https://qmi.ubc.ca/joint-cfref-quantum-projects-announced.

- *Use the National Research Council (NRC) as quantum technology advisors*: When seeking to assist promising companies that are not yet market-proven, it is important to assess candidates technically as well as financially. Under the Industrial Research Assistance Program and other vehicles, the NRC already has a mandate to troubleshoot technologies under consideration from a technical perspective. The government should explicitly formalize and expand the NRC's role as a technical advisor on quantum. The NRC can provide significant value-added advice to both tech providers and users.

- *Optimize investment policy*: As a mid-size country in terms of population, but a large country geographically and in stock of resources, Canada needs foreign investment to develop. However, not all investment is created equal. Larger players from the United States have long acquired promising IP-intensive Canadian companies. For the past 20 years, since the initiation of its "Go Out" policy, China has been buying up companies in strategically important sectors, both from a military and economic perspective. As quantum becomes economically and militarily valuable, there will inevitably be consolidation in the sector. If Canada does not appropriately plan, most of its leading quantum companies could be bought up at cheap prices relative to what the sector will be worth in five or 10 years. After the D-Wave announcement in March, reporters asked Minister of Innovation, Science and Industry François-Philippe Champagne about the government's approach to foreign investment policy. He stated:

  > I'm sure you would expect us to be eyes wide open when it comes to whatever we would need to take in terms of steps to protect … [intellectual property] that has been developed in Canada. We're always out there looking at how we can improve to make sure that new technologies and inventions and improvements and IP that has been developed in Canada stays in Canada.[105]

  In other words, the government is aware of the need for capital, but recognizes the importance of intellectual property and of reinforcing the vibrancy of the Canadian quantum ecosystem. Finding the right balance is essential.

- *Optimize collaboration with global players*: In recent years, the largest technology players globally have become interested in quantum. AWS, IBM, Microsoft, Google, Honeywell and AT&T, among others, are investing in quantum technologies, especially quantum computing. Because of the technology's unsettled nature, some companies are making big bets in specific areas while others seek interoperability (i.e., agnostic). For Canada, there is no specific playbook for global players to work with and how. Building Canadian leaders into global scale companies is undoubtedly a priority. Yet, Canada would also benefit from partnering with global technology leaders. This question should be squarely addressed in the national quantum strategy.

[105] Sean Silcoff, "After a Year of Reset Expectations, D-Wave Secures $40 Million from Ottawa for Quantum Computing," *Globe and Mail*, March 11, 2021, https://www.theglobeandmail.com/business/article-after-year-of-reset-expectations-d-wave-secures-40-million-from-ottawa/.

- *Use large funding envelopes to bring quantum innovators to Canada*: In the quantum economy, Canada is in a global war for talent. The demand for skilled quantum innovators far outstrips supply. As billions of dollars globally are poured into research and development and new companies proliferate, more players will seek out top talent with big pay packages and research budgets. Canada has successfully attracted an array of international quantum researchers. The story of Alán Aspuru-Guzi and Zapata is discussed above. Other examples include David Cory, who went to Waterloo from MIT, and Andrea Damascelli, an Italian who went to UBC from Stanford. Keeping these leaders in the field and attracting others will require an ongoing assessment of Canada's relative attractiveness as a quantum destination. Correspondingly, Canada should become more systematic about whom it pursues and what competitive endowments look like.

- *Partner with major industry associations on use cases*: Many companies face the challenge of not knowing exactly what they would do with a quantum computer. There are many industries in which there are still few to no-use cases exploring how quantum computers could help them with their business. The Canadian government may wish to consider playing matchmaker and underwriter of use cases, between, say, D-Wave, which has an established quantum computer, and large Canadian corporates. An entity such as the Business Council of Canada, which represents the CEOs of the 150 largest companies in the country, could be a good partner in such a venture. Over the medium term, other Quantum Industry Canada members could be included in use cases.

Security

- *Push for NATO and/or Five Eyes collaboration on emerging quantum threats*: Quantum technologies will change the operation and functioning of many aspects of the battlefield. In addition, its medium-term potential to swiftly crack all existing encryption/computer security protocols and upend the world of cyber-security is important for militaries, intelligence services and companies. The 2021 U.S. *National Defense Authorization Act* mandated the creation of a high-level steering group on emerging threats, in which quantum technologies feature prominently. Given China's significant investments and Russia's reasonably well-funded research program, Canada has an interest in extending the emerging quantum threat discussion to its alliance partners.

- *Prepare to pick an investment lane*: The Department of National Defence's Quantum Science and Technology Strategy indicates that it wants to focus its quantum defence research budget in the area of sensors. This focus is appropriately aligned with Canada's spending capabilities. Sensors are also a sound choice. They will be enormously important to the functioning of future battlefield systems and have strong applicability in the civilian world. One need only think of all of the IoT sensors presently installed on power plants, pipelines and other infrastructure to recognize that the demand will be enormous. While it is still early days, DND is thinking about where it wants to place a big bet at an appropriate time. It is appropriate for other parts of the Canadian government to begin similar planning. Presumably, Canada's forthcoming quantum strategy will establish the pathway.

International Co-operation

- *Develop a clear statement of Canadian interests and linkages to co-operation*: Canada has heretofore pushed off structured international co-operation on quantum because it has not had a domestic strategy or a clearly articulated set of interests. While this seems set to change with the National Quantum Strategy process, ensuring an effective understanding of how international co-operation can reinforce Canadian advantages is essential. Not all agreements and partners are beneficial to Canada. Developing a framework for making these determinations is important.

- *Sign a co-operation agreement and develop a detailed action plan with the United States*: The United States and China are the preeminent quantum powers in the world. Given the evolution of geopolitics, China's propensity to target Canadian intellectual property and the strained relations between the two countries, quantum initiatives with China are increasingly off the table. On the other hand, the United States is a long-time friend, partner and ally on economic and security issues. Japan and the U.S. signed a statement of co-operation in December 2019 – the first of what will undoubtedly be a series of international quantum co-operation agreements. In the Canadian case, it would be wise to link a co-operation agreement with a specific action plan which ensures that Canadian interests are reflected and advanced. This could, for example, facilitate Canadian participation, both academic and private sector, in the QIS centres in a way that is not happening much at present.

- *Join the U.S. quantum internet project*: Much of the action in the U.S. private sector is focused on the race to perfect the quantum computer. There is less focus on quantum communications; namely, the quantum internet. China has the rudiments of a quantum internet powered by two satellites and several thousand kilometres of fibre. By linking quantum computers in a quantum internet, the network grows both stronger and more secure. Three essential elements to making this work are (1) quantum key distribution (i.e., securing the endpoints); (2) teleportation of entangled photons (i.e., securing the transmission); and (3) quantum repeaters (i.e., ensuring fidelity by guarding against the degradation of the message over longer distances). Collaborating with the U.S. on these three areas can only benefit Canada.

- *Pursue collaboration agreements with the U.K., Europe and Japan*: As part of the process of developing the U.S. co-operation agreement and action plan, it will be important to know how the U.S. is co-operating with these countries and where their sensitivities are. Just because they are U.S. allies does not mean that the U.S. does not see them as rivals. While Canada would in no way give the U.S. a veto over any quantum co-operation with anyone, the key is to maximize partnerships with like-minded countries without diminishing its (hopefully, expansive) partnership with the United States. Existing initiatives, such as the UBC partnerships with Japanese and German partners, provide important building blocks for what is possible.

Infrastructure

- *Develop a detailed infrastructure plan*: Quantum is expected to significantly change the Canadian technology landscape over the medium term. While we are some years away until quantum technologies become consumer facing on a mass scale, government institutions and major companies will henceforth increasingly adopt these technologies. This is driving the worldwide market projection of US$65 billion by 2030. As this shift occurs, the volume of data that is being created, stored, accessed and transmitted will only accelerate. It is therefore recommended that the government begin preparing for this transformation by undertaking a detailed digital infrastructure plan. It would have two parts: how the federal government needs to prepare; and how major institutions, cities, provinces and society need to prepare. Based on what we know, topics could include:
    - Impact on existing 5G and future 6G cellular networks;
    - Adequacy of existing fibre network;
    - Need to construct new data centres/overhaul (quantum-enable) existing data centres;
    - Importance of space/satellite transmissions to Canada's quantum communications system;
    - Security – and how to start planning.

Conclusion: Towards a New Paradigm

In 1962, American philosopher Thomas Kuhn offered a radical theory for how scientific change occurs. In *The Structure of Scientific Revolutions*, Kuhn argued that change has four stages: (1) the status quo (what Kuhn calls "normal science"); (2) the emergence of anomalies in the status quo (created by what Kuhn calls "extraordinary research"); (3) the crisis in the old model and adoption of a new paradigm; and (4) institutionalization of a new status quo.[106] Applied to contemporary technology, many would see these dynamics as describing the process of what is now called disruption.

While the advancements have been extraordinary, there is no consensus yet on the core methodologies for harnessing quantum phenomena. Yet, the pace of change and the amount of investment show that a vibrant quantum sector is beginning to emerge. As Kuhn would say, the

[106] Thomas Kuhn, *The Structure of Scientific Revolutions* (50th Anniversary Edition), (Chicago: University of Chicago Press, 2012).

progress of the quantum computing revolution is well into the "extraordinary research" phase as the new paradigm's outlines begin to take shape.

The key question for governments in periods of extraordinary technological change is how to position their countries to benefit from these shifts. As Canada considers its strategy, it must consider how quantum intersects with similarly extraordinary technological revolutions in fields such as artificial intelligence, robotics, nanotechnology and genome editing. In no small way, each of these areas is inter-related. Quantum computing, for example, will provide the computing brawn to power the AI-enabled brain in next-generation robots. Any number of these intersections will demand extraordinarily nuanced policies that are permissive of innovation, but consistent with Canadian laws and values. It also will behoove policy-makers to think through the implications of these intersections for areas as diverse as diplomacy, manufacturing and health care.[107]

As technologies mature and are standardized and market consolidation occurs, Canada, like any early leader, risks seeing its early advantages in quantum eroded. Yet, with the steps recommended above and the substantial investments announced in Budget 2021, Canada is poised to remain in a leadership position in quantum throughout the paradigm shift and as the new status quo is institutionalized.

---

[107] Randolph Mank, "Quantum Diplomacy for a New Technological Age," Canadian Global Affairs Institute, December 2017, https://www.cgai.ca/quantum_diplomacy_for_a_new_technological_age.

About the Author

Eric Miller *is a Fellow at the Canadian Global Affairs Institute and President of Rideau Potomac Strategy Group. Mr. Miller advises private and public sector clients on North American, Asian, Latin American, and European technology, trade, economic and geo-political matters. He previously served as Vice President for North America and Cybersecurity at the Business Council of Canada and as the first representative of Canada's Department of Industry in the United States, based at the Canadian Embassy in Washington, DC. He has advised the Government of Canada on strategic matters related to the quantum technology policy.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.