TECH FACTSHEETS FOR POLICYMAKERS

SPRING 2020 SERIES

Quantum Computing

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

AUTHOR

Akhil Iyer (Harvard)

EDITOR AND CONTRIBUTORS

Emma Rosenfeld (Harvard)
Mikhail Lukin (Harvard)
William Oliver (MIT)
Amritha Jayanti (Harvard)

The Technology Factsheet Series was designed to provide a brief overview of each technology and related policy considerations. These papers are not meant to be exhaustive.

Technology and Public Purpose Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street, Cambridge, MA 02138

www.belfercenter.org/TAPP

Design and layout by Andrew Facini

Printed in the United States of America

Executive Summary

Quantum computing refers to the use of quantum properties—the properties of nature on an atomic scale—to solve complex problems much faster than conventional, or classical, computers. Quantum computers are not simply faster versions of conventional computers, though they are a fundamentally different computing paradigm due to their ability to leverage quantum mechanics. Harnessing quantum properties, namely the ability for the quantum computer bits (called "qubits") to exist in multiple and interconnected states at one time, opens the door for highly parallel information processing with unprecedented new opportunities. Quantum computing could potentially be applied to solve important problems in fields such as cryptography, chemistry, medicine, material science, and machine learning that are computationally hard for conventional computers. Although it is still unclear which specific tasks can benefit from parallelized quantum processing, known as quantum parallelism, it is expected that solutions to a number of problems, especially those related to optimization, can be greatly accelerated by using a quantum computer.[1]

Though the field is still in its early stages, the anticipated opportunities offered by the unique computational power of quantum computers have attracted investment from not only research universities, but also startups, technology giants like Google, IBM and Microsoft, and directed investment by governments around the world.[2] This cross-sectoral ecosystem has supported recent progress in underlying hardware, software, and algorithms necessary to make the computers work. The field has seen rapid advancement, however systems that can accomplish various kinds of computation, and especially those that can be commercially viable, are still likely to be decades away.[3] There are expected to be some near-term applications on the horizon though, making quantum computing as relevant as ever.

Currently, U.S. governance and regulation regarding quantum computing—a subset of the broader field of **quantum information science**, which also encompasses quantum communication and quantum sensing—focus on investments in the technical knowhow, collaborative research ecosystem, and human capital required to advance the technology. Given quantum computing's potential for impact, especially in the fields of digital security, healthcare, energy, and machine learning and artificial intelligence, it is important for policymakers to understand the likely trajectories of the technology over the coming decades, as well as the pace of development both within the U.S. and abroad. Furthermore, policymakers must consider how to effectively promote the development, application and implementation of general-purpose quantum technologies to realize their larger economic and social benefits, while simultaneously mitigating foreseeable risks to privacy, safety, security, and inclusion.[4]

---

[1] National Academies of Sciences, Engineering, and Medicine. (2019). *Manipulating Quantum Systems: An Assessment of Atomic, Molecular, and Optical Physics in the United States.* Washington, DC: The National Academies Press. https://doi.org/10.17226/25613

[2] Gibney, Elizabeth. "Quantum Gold Rush: the Private Funding Pouring into Quantum Start-Ups," October 2, 2019. https://www.nature.com/articles/d41586-019-02935-4.

[3] Oliver, William. *Quantum Computing Primer*, 2019. https://events.technologyreview.com/video/watch/william-oliver-quantum-computing-primer.

[4] Denning, Dorothy E. "Is Quantum Computing a Cybersecurity Threat?," June 14, 2019. https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat.

What is Quantum Computing?

Quantum computing, a subfield of quantum information science (an area of study based on the idea that information science depends on quantum effects in physics), can be defined as the use of quantum properties to solve complex problems much faster than conventional, or classical, computers. Underlying quantum technology is a fundamentally different way of storing and manipulating information, as compared to conventional computers. Where conventional computers use "bits," or binary digits that are the basic unit of computer information storage and processing, quantum computers use quantum bits ("**qubits**").[5] There are significant differences between bits and qubits: Bits are similar to switches—they can be either up or down, on or off. Qubits, though, are more like dimmer knobs—they can take on an infinite number of different values between on and off, and this, along with other mechanical properties, underpins their computational functionality.[6]

Quantum computing takes advantage of two mechanical phenomena of qubits. The first is **superposition**, in which qubits can exist simultaneously as both a "0" *and* a "1". This is unlike classical computers, in which a bit can only assume one state at a time—either being a "0" *or* "1". By being able to simultaneously exist in both states, quantum computers are able to encode multiple paths of computation at any given moment.[7]

The second related phenomenon, **entanglement**, is where qubits act as a group with measurable interconnectedness—qubits are "entangled" with one another. Entanglement between qubits is a key resource of quantum computing, as it allows the qubits themselves to share information, and enables the computer to explore and manipulate a much larger quantum state space which is hidden from classical computers. As more qubits are added to a quantum computer system, their entanglement and interference between their superposition states enables them to simultaneously process multiple options for the computation at speeds significantly, sometimes exponentially, faster than conventional computers.[8]

One way to conceptualize some of the differences between conventional and quantum computing is through a simplified example of both platforms attempting to solve a complex maze: A conventional computer would *sequentially* attempt every possible path until it reaches the correct option. A quantum computer, on the other hand, can exploit its ability to represent multiple states at any given moment and test all pathways *simultaneously,* allowing to quantum interference of different pathways and thus achieving its solution in a far shorter period of time. This is the essence of **quantum parallelism**, or the ability

---

[5] Accessed 2020. https://quantumatlas.umd.edu/entry/Qubit.

[6] Ibid.

[7] "Quantum Computing 101," Institute for Quantum Computing, May 17, 2013, https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101.

[8] "Quantum Computing | Microsoft," Microsoft Quantum - US (English), https://www.microsoft.com/en-us/quantum/.

for a quantum computer to simultaneously evaluate multiple values for a given function, which can be achieved due to the phenomena of superposition and entanglement.[9] In classical computers, there exists the capacity to run parallel processes, but this requires scaling hardware and memory—different sets of computer bits would be required to achieve parallel processing.[10] In that sense, quantum demonstrates a possible advantage in reducing resources needed to run parallel computations because the *same* qubits can be used at any given moment to execute various computational paths.[11]

Designing quantum algorithms that demonstrate a quantifiable improvement in speed compared to conventional computers is an ongoing and significant challenge. The theoretical field of quantum algorithms attempts to design protocols that capitalize on the quantum properties of superposition, entanglement and quantum interference, while proving a demonstrable advantage over the best existing classical algorithms.[12]

It is important to note, though, that not all use cases of quantum computing will likely display an inherent **quantum advantage** (also known as **quantum supremacy**), in which a quantum computer demonstrates significant advantages in processing time over its conventional counterparts.[13] There may be cases where classical computers are still the optimal tools to address computational problems, particularly in the near- and mid-term.

Classes of Quantum Computing

Three broad classes of quantum computers exist in harnessing quantum properties for computation, with varying degrees of known utility and technological availability: universal fault-tolerant quantum computers, quantum annealers, and noisy intermediate-scale quantum (NISQ) devices.[14]

The ultimate goal of quantum computing is to develop a **Universal Fault-Tolerant Quantum Computer**. A large-scale universal fault-tolerant quantum computer would harness immense computational capability, but today remains a distant prospect given the technical challenges associated with connecting thousands of fault-tolerant qubits without disturbing their quantum properties. Another class of quantum computing is **Quantum Annealers**, which leverages quantum principles to target optimization problems (e.g. fastest travel route). It has yet to be determined whether annealing exhibits a quantum advantage over classical computing for most problems.

---

[9] National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum Computing: Progress and Prospects.* The National Academies Press, Washington, DC. doi: https//doi.org/10.17226/25196

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Quantum Computing Primer, (2019).

The most relevant to current quantum computing development are **Noisy Intermediate-Scale Quantum (NISQ)** devices. These devices seek to target problems that emulate inherent quantum properties themselves (such as understanding the complex nature of molecules), as well as optimization problems. While limitations exist in their application, some NISQ devices represent the most technologically advanced form of quantum simulators today, in which known and likely advantages exist over classical computing despite their "noisy," or error-prone nature.

Important features of a NISQ Computing System

Qubit arrays: Quantum bits represent the fundamental building block of quantum computing. Unlike classical bits, which store the value of 0 or 1 within a transistor, qubits carry its information within the states of the quantum particles, which can be an atom, ion or a small superconducting electrical circuit. Most importantly, qubits leverage the quantum principles of existing in multiple states (superposition), in conjunction with inter-relatedness between qubits (entanglement), to increase a computer's speed.[15]

Supporting control systems: Qubits are extremely sensitive to vibrations and other noisy environmental disturbances that can disrupt their superposition state. This requires robust and specialized hardware to establish and maintain these states. Varying methods to achieve control and maintain these states exist, and they differ based on the type of physical system used to store quantum information.

Technical Challenges & Limitations

While quantum computing has gained immense interest, significant challenges exist in bringing the technology to full fruition. Some of the greatest challenges at present include:

- **Scaled Qubit Systems**: Controlling, interconnecting, and reading out qubits as the number of qubits increases is very challenging. Additionally, in order to access the full quantum state space available to a quantum computer but hidden to a classical computer, all qubits must become entangled with each other. As the numbers of qubits increases, the number of pairs of qubits increases quadratically. Achieving so-called 'all-to-all connectivity' imposes stringent technical requirements and limitations on the hardware geometry, size, and physics.

- **Control Systems:** Conducting operations in a computation, without introducing errors, is an ongoing area of research. In practice, when manipulating qubits under a desired operation, the qubit evolution and final state is not perfect due to control errors or loss of coherence. In particular, employing quantum error correction appends many quantum operations to a computation, thereby compounding control errors.

- **Maintained Coherence**: The coherence time of qubits quantifies the time in which a system maintains its quantum state. The longer the coherence time, the more operations a quantum computer can execute. Improving coherence is critical to realizing the full benefits of quantum computing power. But improving coherence time can be extremely difficult given the

---

[15] Quantum Computing 101, (2013).

sensitivity of a quantum system to the noise of environmental disturbances like vibration, temperature changes or electromagnetic waves.[16]

- **Near-Term Error Mitigation Versus Long-Term Error Correction**: Error correction helps combat the loss of coherence by leveraging some qubits to correct errors made by other qubits actually executing the calculations, or by using multiple qubits to encode the same information. In terms of hardware, the technology remains nascent at best; one analyses suggests that in the near-term, one fault-tolerant qubit would require a supporting cast of nearly 1,000 error-correcting qubits to be effective.[17] Alternative, error-correcting techniques are under development as a means to extrapolate results within different types of noisy environments.[18]

- **Scaled Data Input:** Though the advantage of quantum computers to use a small number of qubits to represent an exponentially larger amount of data exists, there currently is no method to efficiently transform a large amount of classical data into a quantum state (unless the data can be generated algorithmically, in which case there is no need for a classical-to-quantum conversion).[19] This is a significant limitation for quantum computing applications considering existing information bases are stored mostly in classical form.

- **Algorithm Design**: Measuring the state of a quantum computer essentially takes a snapshot of the large quantum state and condenses it into a single classical result. This means that observers can only collect the same amount of data from a quantum computer that can be collected from a classical computer of equivalent size.[20] To capitalize on the benefits of this technology, algorithms for quantum computers must be designed in a way that take advantage of uniquely quantum characteristics. This is a complex problem that highlights the foundation differences between classical approaches and quantum approaches to computation.[21]

- **Quantum Software Stacks**: Since quantum programs are different from classical programs, it is necessary for new systems to be developed to support the effective execution of hardware, such as creating and debugging (removing software errors) quantum-specific software.[22] Developing software to support existing hardware helps create a feedback cycle between the two components of quantum machines in a way that helps improve both by highlighting component-specific issues. The development of effective software stacks to support quantum hardware is still an early, iterative and open challenge.[23]

Developments in the parallel fields of quantum communication and quantum sensing, as well as advancements in other technologies like photonics, semiconductors and refrigeration, all together contribute to the pace of quantum computing developments.

---

[16] Coles, Scott Pakin, Patrick. “The Problem with Quantum Computers.” June 10, 2019. Scientific American Blog Network. https://blogs.scientificamerican.com/observations/the-problem-with-quantum-computers/.

[17] Phillipp Gerbert and Frank Ruels. “The Next Decade in Quantum Computing—and How to Play.” Boston Consulting Group. November 15, 2018. https://www.bcg.com/en-us/publications/2018/next-decade-quantum-computing-how-play.aspx

[18] Naomi H. Nickerson and Benjamin J. Brown. “Analyzing correlated noise on the surface code using adaptive decoding algorithms.” Quantum Journal, Volume 3. 2019. 131.

[19] Quantum Computing: Progress and Prospects, (2019).

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Ibid.

Applications and Market Development

While a variety of technical challenges remain in developing practical quantum computing capabilities, the technologies' ultimate development could apply to many aspects of computation, regardless of industry or field. Near-term uses of quantum computing technologies could leverage a combination of quantum and conventional computer systems working together in an effort to realize efficiency gains in certain problems.[24]

Though there are many expert predictions on the **timelines for advances in quantum computing** and its applications (e.g. seeing potential tangible applications to cryptography in the 10 to 20-year time horizon), the real timeline is uncertain.[25] Due to increasing progress in the field though, the foreseeable real-world applications are becoming more realistic and are likely to be on the horizon. As quantum technology improves, some technologies, methods and activities with the potential to witness advancement by quantum computing include:

- **Modeling Quantum Systems:** Quantum computers present a unique opportunity to enhance scientists' ability to better model the quantum mechanics that dictate how biomolecular and material systems work.[26] By better understanding these systems, scientists and engineers can apply new knowledge to the fields of chemistry, biophysics, material design, and more.

- **Material Science:** Quantum computing holds the potential to be applied to model the reactions and aging of materials, such as battery cells for energy advancements.[27] Applications of quantum technology to material science could have significant impacts on the development ceramic and glasses, polymers, composites, metal alloys, and semiconductors—all important industrial components.

- **Biophysics and Chemistry:** As referenced previously, knowledge gained for modeling quantum systems can be applied to fields such as biophysics and chemistry. These applications have their own potential outcomes by leverage quantum computing, such as finding the most likely configuration of molecules or chemical processes for understanding chemical reactions; or simulating the complex nature of large, individual molecules (e.g. enzymes) to understand their properties and reactivity, and ultimately engineer composite materials and new pharmaceuticals.[28] This could have large implications for the healthcare industry.

- **Machine Learning/Artificial Intelligence:** Quantum's inherently probabilistic way of solving could lend utility to expanding the process of machine learning through the development of quantum neural networks, in particular for problems

---

[24] Andrew Fursman and Arman Zaribafiyan. "Innovating with Quantum Computing." Accenture. 2017. https://www.accenture.com/t00010101T000000__w__/br-pt/_acnmedia/PDF-45/Accenture-Innovating-Quantum-Computing-Novo.pdf

[25] Quantum Computing: Progress and Prospects, (2019).

[26] Quantum Computing Primer, (2019).

[27] Quantum Computing Primer, (2019).

[28] Aspuru-Guzik, A. et al. (2019). Quantum Chemistry in the Age of Quantum Computing. Chemical Reviews. Volume 119, Issue 19. 10803-11006.

involving quantum systems.[29] In looking at near-term applications, significant attention has surrounded the horizontal integration opportunities within artificial intelligence technologies.[30] This is due to the expectation held by some scientists that quantum-based machine learning systems can train on data sets significantly faster than their conventional cousins.[31] However, further advances in quantum algorithms will be required to quantify exactly if and how advantageous quantum devices could be, including addressing unresolved challenges such as loading large datasets into the quantum computer which itself can be time-consuming.

- **General Optimization Problems:** From transportation and logistics to financial modeling, all industries face unique problems of optimization. For example, in finance it could be efficiently evaluating the variety and probability of financial outcomes with an extremely large number of scenarios. Quantum computing, through its ability to exponentially scale parallel processing, demonstrates potential for solving a range of industry-specific optimization problems.[32]

- **Cryptography:** The ability to de-crypt information that employ widely used public key encryption techniques increases exponentially if major advances in fault tolerant quantum computing technology develops. But simultaneously, quantum computing can be leveraged to develop tamper-proof quantum communications networks.[33]

Market Development

Despite the technical challenges and generally long-term estimate for widespread benefits, many leading technology companies and governments are investing heavily in quantum computing, including hardware and software underpinning the technology. The foundational base of quantum development also includes research at universities and national laboratories, such as **Harvard Quantum Initiative**, **MIT Center for Quantum Engineering**, **University of Maryland's Joint Quantum Initiative**, **MIT's Lincoln Laboratory**, and **Sandia National Laboratories**. In addition to academic support and some backing by the venture capital community, companies have sought partnerships with leading firms in the finance, energy, pharmaceutical, automotive and aviation industries, which seek to capitalize on the anticipated benefits of quantum computing.[34] Table 1 lists some of the ongoing cross-sectoral research and development in the field.

---

[29] Iris Cong, et al. "Quantum Convolutional Neural Networks." Nature Physics. Volume 15. 2019. 1273-1278.

[30] Hartmut Neven. "American Innovation in the Quantum Future." CSIS. January 29, 2020. https://www.csis.org/events/american-innovation-quantum-future

[31] Maria Schuld. "Machine Learning in Quantum Spaces." March 13, 2019. Nature. https://www.nature.com/articles/d41586-019-00771-0

[32] Ibid.

[33] Aram Harrow, et al. "Simulating large quantum circuits on a small quantum computer." https://quics.umd.edu/events/simulating-large-quantum-circuits-small-quantum-computer

[34] "Quantum Gold Rush: The Private Funding Pouring into Quantum Start-Ups." October 2, 2019. https://www.nature.com/articles/d41586-019-02935-4.

Table 1: Collaborative Development for Quantum Computing (Representative/Non-exhaustive)

Companies Developing Quantum Hardware	Academic/Public-sector Collaborators	Private-sector Collaborators
IBM[35]	University of Melbourne, Oak Ridge National Laboratory, University of Oxford, Los Alamos National Laboratory, National Taiwan University	JP Morgan, Goldman Sachs, Barclays, ExxonMobil, Samsung, Dupont, Daimler, Mercedes-Benz, Raytheon, Delta Airlines
Google[36]	University of Waterloo, Oak Ridge National Laboratory, NASA, University of California Santa Barbara	Daimler, Volkswagen
Microsoft[37]	Purdue University, Case Western Reserve University, Pacific Northwest National Laboratory, University of Sydney, Technical University of Copenhagen, Eindhoven University of Technology, University of California Santa Barbara, University of Sydney	Honeywell, Dow, Ford, 1QBit, Bohr Technology, Cambridge Quantum Computing, Entropica Labs, GTN, OTI Lumionics, ProteinQure, QC Ware, Qulab, QxBranch, Riverlane Research, Solid State AI, Strangeworks, and Zapata Computing
Intel[38]	University of Toronto, University of Chicago, Delft University of Technology	
Biogen[39]		Accenture Labs, 1QBit
D-Wave[40]	University of Waterloo, Los Alamos National Laboratory, Oak Ridge National Laboratory	Google, Lockheed Martin, Volkswagen, Amazon Web Services; NEC Corporation
Honeywell[41]		Microsoft, JP Morgan
Rigetti[42]	UC Berkeley	Amazon Web Services
Alibaba[43]	University of Science and Technology of China, Chinese Academy of Sciences	

Particularly critical to the quantum eco-system are the developers and suppliers of key hardware components. This includes not only major semiconductor and silicon-based technologies, but also more specialized components, such as specialized vacuum chambers and optics packages from manufacturers like **Cold Quanta**[44], as well as dilution refrigerators for super-conducting systems made by companies

---

[35] Chris Fisher Abenojar Eric, "IBM Q Network | Members," 02019-04-02, www.ibm.com/quantum-computing/network/members.

[36] "Forbes: NASA and Google Partner to Work With a D-Wave Quantum Computer | D-Wave Systems," https://www.dwavesys.com/press/forbes-nasa-and-google-partner-work-d-wave-quantum-computer.

[37] "Quantum Computing | Microsoft."

[38] "Intel Labs Partnerships - Driving Research Through Collaboration," Intel, https://www.intel.com/content/www/us/en/research/partnerships.html.

[39] "Advancing Drug Discovery through Quantum Computing." Accenture. Accessed 2020. https://www.accenture.com/us-en/success-biogen-quantum-computing-advance-drug-discovery.

[40] "Customers | D-Wave Systems." Accessed 2020, https://www.dwavesys.com/our-company/customers.

[41] "Quantum | Honeywell." Accessed 2020 https://www.honeywell.com/en-us/company/quantum

[42] "Rigetti Computing," Rigetti Computing. Accessed 2020 https://www.rigetti.com/community.

[43] "Alibaba Lays Out Roadmap for Frontier Technology Research - DAMO Academy," Accessed 2020, https://damo.alibaba.com/events/38.

[44] "Cold Quanta Products." Accessed 2020, https://www.coldquanta.com/standard-products/

like **Bluefors** in Finland.[45]

An array of firms developing quantum software based on the varying hardware approaches has also emerged, with startups like **Zapata Computing**, **1Qbit**, **Strangeworks**, **QC Ware** and **QxBranch**.[46] The development cycle is for quantum computing is longer as compared to classical computing applications, and therefore startups and smaller ventures are in a unique position for funding, needing to demonstrate consumer applications and promise over an investor-friendly timescale. This is a consideration less relevant in certain industries though, such as pharmaceuticals, since the research, development and production timescale are traditionally longer anyway.

Public Purpose Considerations

Near-Term: Funding, Workforce Training, Collaborations, and Security Implications

The majority of near-term challenges surrounding quantum computing reflect the approaches by which to collaborate and foster the quantum research ecosystem, particularly as it relates to technological advancement, talent and the sharing of near-term applications.

- **Funding Ecosystem:** The funding ecosystem for quantum computing is composed of a mixture of private and public financing.[47] Funding sources for the development and application of technologies have associated incentive structures that have large influence over what initiatives within a field of technology get prioritization. As the field of quantum computing continues to grow, the amount of government funding is not concurrently increasing.[48] It is important for policymakers to consider how a gap in public funding could impact the development and application trajectory of quantum computing technology. Relatedly, it is valuable to consider what role the government should play in the foundational resource support of this cutting-edge field.

- **Education & Workforce Development:** A well-trained and growing workforce is foundational for the progression of research and development in the field of quantum computing.[49] In particular, attracting and retaining the top talent, training future quantum scientists in relevant skills for industrial applications and bridging the academic-industrial gap is an increasing necessity. Policymakers must consider how to develop a sustainable and scalable pipeline for a workforce trained in quantum computing and engineering. It is also important for policymakers to consider how to encourage

---

[45] Quantum Technologies Overview. 2016. http://theory.caltech.edu/~preskill/talks/qTechIQIMretreat2016-v2.pdf

[46] Stephen Gossett. "20 Quantum Computing Companies to Know." February 24, 2020. https://builtin.com/hardware/quantum-computing-companies

[47] Manipulating Quantum Systems: An Assessment of Atomic, Molecular, and Optical Physics in the United States, (2019).

[48] Ibid.

[49] Ibid.

diversity and inclusion within the workforce (based on race, gender, socioeconomic status, education, ethnicity, and more), as this directly impacts the progression and culture of quantum computing as a field.

- **Cross-Sector Collaboration:** Collaboration between different sectors on quantum computing, particularly between academia and industry, will be (and already is proving to be) essential for rapid advancement of quantum computing science and technology. The fast-changing nature of the field, requiring a combination of cutting-edge basic science and state of the art technology, requires close collaboration between leading academic groups, national laboratories, start-ups and larger companies. This raises important considerations around intellectual property (IP) rights between various stakeholder groups, such as academia, industry and national labs. It is essential for policymakers to consider how to develop and implement an approach that strikes a balance between open and distributed intellectual ownership, and the fair distribution of resources and profits.

- **International Collaboration:** Through knowledge sharing, international collaboration on basic research in quantum computing is necessary to facilitate breakthroughs within the field. The U.S. scientific community already engages in international collaboration with research groups in the European Union, United Kingdom, Canada, Japan, Australia, China, and others.[50] Federal initiatives for the research and development of quantum computing are, in part, motivated by national competitiveness, though. It is important to understand how the U.S. can continue open international collaboration on foundational quantum computing research, while still considering national security, strategy, and competitiveness.

- **Encryption and Security Infrastructure:** Implementing encryption standards for potential future challenges from quantum computer advancements represents a growing concern. Tools for quantum resistant encryption are being developed by the National Institute for Standards and Technology (NIST).[51] Implementing quantum resistant encryption proactively could be difficult. Policymakers must consider how to incentivize a wide-scale adoption of new encryption standards to ensure the security of internet systems once quantum computers are able to challenge the existing encryption protocol.

Long-Term: Cybersecurity, Ethics of Artificial Intelligence, and Accessibility

- **Cybersecurity:** Heightened interest in the risk posed by quantum computing to cybersecurity followed the publication of Peter Shor's famous 1994 quantum algorithm, which theorized the ability of a large and relatively error-free quantum computer to break current public key encryption standards. Today's public key infrastructure, to include common RSA encryption protocols, rely on the fact that a classical computer can easily multiply large prime numbers but have immense difficulty breaking down this mathematical product without a key. But a large, fault-tolerant quantum computer could theoretically factor a very large number in a dramatically shorter period of time and render many of today's common encryption standards obsolete.[52]

- **Ethics of Artificial Intelligence:** Because quantum computing has the potential to enhance the pace of artificial intelligence development, the same public purpose considerations and concerns exhibited by the application of artificial intelli-

---

[50] Ibid.

[51] Robin Materese. "NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals.'" Text. NIST, January 30, 2019. https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals.

[52] Is Quantum Computing a Cybersecurity Threat?, (2019).

gence also exist within quantum computing. These include concerns like transparency and interpretability, discrimination and bias, privacy and security, fairness, and trustworthiness.[53]

- **Accessibility and Inclusion:** Government plays a key role in shaping industry engagement with, and establishing appropriate mechanisms for, resource and infrastructure distribution. This was true for classical computers and the internet (among other foundational technologies) and will most likely be true for quantum computers.[54] Accessibility to the benefits of quantum computing is a public purpose consideration that must be intentionally addressed by policymakers. Similar considerations that are also relevant to the development of quantum internet, involving quantum computers connected through quantum channels, with absolute security guaranteed through quantum encryption.[55] Policymakers must consider who reaps the benefits of quantum technology, and what role various stakeholders have in ensuring accessible and inclusive positive outcomes.

- **Economic and Social Change:** Quantum computing, once technologically mature and commercially viable, is posed to revolutionize nearly every industry much like classical computers have done.[56] Considering how quantum computers could catalyze grand shifts in economic and social landscapes is important in understanding how and why to invest in the technology, and what governance schemes should be implemented to maintain public values, such as privacy, safety, security, diversity, fairness, and more.

---

[53] Müller, Vincent C. "Ethics of Artificial Intelligence and Robotics," April 30, 2020. https://plato.stanford.edu/entries/ethics-ai/.

[54] Altman, Drew E., John M. Benson, Marcus D. Rosenbaum, Minah Kim, Mollyann Brodie, Rebecca Flournoy, and Robert J. Blendon. "Whom to Protect And How: The Public, the Government, and the Internet Revolution," July 28, 2016. https://www.brookings.edu/articles/whom-to-protect-and-how-the-public-the-government-and-the-internet-revolution/.

[55] Manipulating Quantum Systems: An Assessment of Atomic, Molecular, and Optical Physics in the United States, (2019).

[56] Quantum Computing: Progress and Prospects, (2019).

Current Governance and Regulation

Much of existing policy attention surrounds research and development strategy rather than governance. Below are some of the existing legislation and initiatives regarding the broad category of Quantum Information Science. This discipline includes not only quantum computing, but also quantum communications and quantum sensing, both of which also leverage quantum principles to advance security and measurement accuracy, respectively.

U.S. Legislation & Governance

- **National Defense Authorization Act (2020)**: Establishes an Air Force Quantum Information Science Innovation Center as part of a broader defense effort to accelerate research, while also coordinating with the National Quantum Coordination Office "for workforce development, enhancing awareness and reducing risk of cybersecurity threats, and the development of ethical guidelines for the use of quantum technology."[57]

- **National Quantum Initiative Act (2019)**: Aims to bring a coordinated, ten-year national strategy to support quantum technologies with approximately $1.275 billion in total funding for the next five years**.** The Act, facilitated by Executive Order 13885 that establishes a National Quantum Initiative Advisory Committee under the Office of Science and Technology Policy (OSTP), provides a framework and investment mechanism through which the National Science Foundation, National Institute for Standards and Technology (NIST), and Department of Energy (DoE) can support research, development and application of quantum technology. The law also directs DoE to establish multiple National Quantum Information Science Research Centers. Finally, the Act requires NIST to support "human resources development in all aspects of quantum information science" as well as identify future cybersecurity standards that support robust quantum developments.[58]

- **National Strategic Overview for Quantum Information Science (2018):** Strategy developed by the National Science and Technology Council's Subcommittee on Quantum Information Science. Pillars of the strategy include a fostering science-first approach for core research, creating a quantum-smart workforce, deepening engagement with industry, providing critical infrastructure to support research and application, and advancing international cooperation.[59]

- **Executive Order 13702 (2015)**: Precursor to the National Quantum Initiative Act that aimed to advance U.S. leadership in the quantum field by establishing a National Strategic Computing Initiative.[60]

---

[57] "Quantum Computing in Cyber Security Domain: Report and HSD Cafe," September 18, 2019, https://www.thehaguesecuritydelta.com/news/newsitem/1345-quantum-computing-within-the-security-domain-report-launched.

[58] Lamar Smith, "H.R.6227 - 115th Congress (2017-2018): National Quantum Initiative Act," webpage, December 21, 2018, https://www.congress.gov/bill/115th-congress/house-bill/6227.

[59] National Strategic Overview for Quantum Information Science. National Science and Technology Council. September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf

[60] "National Strategic Computing Initiative (NSCI)," https://www.nitrd.gov/nsci/.

U.S. Bilateral Agreements

- **Japan:** Tokyo Statement on Quantum Cooperation (2019), in which both countries intend to embark on good-faith cooperation in quantum information science and developing the next generation of scientists.[61]

- **U.S. Funded Collaboration:** While not itself a standalone agreement, the U.S. government does financially support and collaborate with key allies in quantum technologies (e.g. Australia).[62]

International Governance Schemes

- **Australia**: In 2017, the Australian Research Council (ARC) funded the Centre for Quantum Computation and Communication Technologies through its Centre of Excellence Program. The Centre has received $33.7 million over seven years, and is led by the University of New South Wales.[63]

- **Canada**: In 2019, the Canadian government began implementing a $41 million initial investment to foster a Quantum Valley eco-system centered around the University of Waterloo, a leading research hub for quantum information science.[64]

- **China:** Beginning in 2017, China undertook significant efforts to fund and establish its own Quantum national laboratory. With an initial $1 billion investment and an anticipated $9 billion additional forthcoming, President Xi Jinping has challenged China's National Laboratory for Quantum Information Sciences, as well as associated institutions like Alibaba's Shanghai Quantum Lab, to achieve significant quantum breakthroughs by 2030.[65]

- **European Union:** Beginning in 2016, the European Union began developing its Quantum Technologies Flagship. With a ten-year mandate, the flagship program is expected to receive approximately $1 billion Euro's in support. [66]

- **India**: India established its National Mission on Quantum Technology and Applications, with recent 2020 public proposals to invest $1.2b.[67]

- **Japan:** In late 2019, the Japanese government released a roadmap to advance national quantum computing research and initiatives. The government is providing $276 million in funding for quantum research for the fiscal year beginning April

---

[61] "Tokyo Statement on Quantum Cooperation," *United States Department of State* (blog), https://www.state.gov/tokyo-statement-on-quantum-cooperation/.

[62] The University of Sydney. "US Government Major Investment in Quantum Technology." May 3, 2016. https://www.sydney.edu.au/news-opinion/news/2016/05/03/us-government-major-investment-in-quantum-technology.html.

[63] Quantum Computing: Progress and Prospects, (2019).

[64] "Government of Canada partners with digital industries to invest in ground-breaking technology and businesses." April 18, 2019. https://www.canada.ca/en/innovation-science-economic-development/news/2019/04/government-of-canada-partners-with-digital-industries-to-invest-in-ground-breaking-technology-and-businesses.html

[65] Abenojar, "IBM Q Network | Members." https://www.ibm.com/quantum-computing/network/members/

[66] "EU Funded Projects on Quantum Technology," European Commission. October 29, 2018, https://ec.europa.eu/digital-single-market/en/projects-quantum-technology.

[67] "FM's Rs 8,000 Crore Boost Will Help India Bridge Gap in Quantum Computing with US, China - The Economic Times," https://economictimes.indiatimes.com/tech/hardware/fms-rs-8000-crore-boost-will-help-india-bridge-gap-in-quantum-computing-with-us-china/articleshow/73835819.cms.

2020. Quantum computing will also be a focus of Japan's "moonshot" research and development program in which the government will invest a total of $920 million.[68]

- **Russia:** In late 2019, Moscow allocated $790 million over the next five years for basic and applied quantum research at its national laboratories.[69]

- **United Kingdom:** In 2014, the United Kingdom's Engineering and Physical Sciences Research Council launched a coordinated national initiative to support and accelerate the development of quantum technologies. The UK National Quantum Technologies Program received £120 million over 5 years for its first phase, and another £94 million in 2019 for its second phase.[70]

---

[68] Dargan, James. "Land of the Rising Qubit: Japan's Quantum Computing Landscape," January 25, 2020. https://thequantumdaily.com/2019/12/09/quantum-computing-japan-land-of-rising-qubit/.

[69] Quirin Schiermeier, "Russia Joins Race to Make Quantum Dreams a Reality," *Nature* 577, no. 7788 (December 17, 2019): 14–14, https://doi.org/10.1038/d41586-019-03855-z.

[70] "Home - UK Quantum Technology." Accessed 2020. http://uknqt.epsrc.ac.uk/.

Appendix: Key Questions for Policymakers

Funding Ecosystem

- How can the U.S. develop an investment scheme, shared by public and private actors, that sustains the research and development of quantum computers and related technologies?

- How should the investment scheme be incentivized and shared amongst cross-sectoral actors, such as large tech firms, the government, venture capital firms, and foundations?

- How can long-horizon funding schemes ensure that they are continuing to support cutting-edge research in quantum technology, such as enhanced control systems for cold atoms and molecules, that are critical to the progress of quantum computing?

- How do we protect the intellectual property of the innovative hardware and software stemming from quantum computing (in order to incentivize research and investment), while allowing for open and collaborative eco-systems necessary for progress and development?

Education & Workforce Development

- How can policymakers foster and retain a larger talent pool of quantum information expertise? (i.e. H1-B visas, hiring authorities, etc.)

- How can academic institutions increase their capacity to hire and support faculty and staff within the field of quantum computing?

- What do academic institutions need to do to establish clear pathways for students to pursue a degree in quantum computing and engineering?

- How can the U.S. government help foster and encourage an ecosystem of diverse (by gender, race, ethnicity, socioeconomic status, and more) and inclusive talent development in the field of quantum computing?

- How can the field of quantum computing draw on the overarching science, technology, engineering and mathematics (STEM) talent pool that is growing with in the U.S. and internationally?

Technical Development & Efficacy

- How do we best distribute and prioritize resources allocated by the National Quantum Initiative Act across the three major areas of quantum information science, to include quantum computing, quantum sensing and quantum communication?

- How do we promote and assess the value, utility, and long-term strategy of partnerships between federally funded research centers and industry?

- How can we develop more collaborative research efforts with other nations in the field of quantum computing, as demonstrated by the recent U.S. agreement with Japan? What benefits and challenges arise in similar agreements with other countries? How do we promote open collaboration in basic research without compromising security given the ongoing interdependencies in the technological and supply chain eco-system?

- How can we characterize the development of associated technologies that underpin the advancement of quantum computing? What aspects of their development contribute to accelerating or constraining quantum computing advancements?

- How do we measure pace and assess the strategy of our quantum initiatives? How can this inform impact foreseeability and mapping?

Security & Privacy

- What are the challenges in implementing a higher standard of encryption today if we are to hedge against the theoretical risk that quantum computing poses to cybersecurity in the future? What are the broader challenges of implementing post-quantum cryptography or quantum cryptography from an international construct?

- How would the introduction of quantum computing impact the future of warfare and national security?

- How would potential advances in machine learning and artificial intelligence impact privacy and security considerations?

Accessibility & Inclusivity

- How to we ensure the benefits from quantum computing and its applications are shared with the broader public?

- What mechanisms are in place against the monopolization of quantum computation resources? Is there enough of a fair competitive market landscape for quantum research, development and deployment?

Long-Term Economic & Social Impacts

- How do we promote realistic understanding of the opportunities and challenges in quantum computing?

- How can policies be proactive about foreseeable security and privacy concerns while still maintaining a curiosity-driven research and development ecosystem?

- How can policy and governance schemes promote other public purpose considerations, such as safety, diversity, inclusion, fairness, equity at early stages of quantum development such that long-term economic and social impacts of quantum computing embody these principles? How do all components of progress, from funding schemes to workforce training to technical development and efficacy play a role the promotion and embodiment of public values?