ATARC

Demystifying the Capabilities of Quantum Technologies Available Today and in the Future

A Compilation of White Papers

February 2025

ATARC Global Quantum Working Group
Copyright © ATARC 2025

Table of Contents

Disclaimer*: This white paper was prepared by the ATARC Quantum Working Group members in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with. This white paper is intended to be a helpful guidance relating to current quantum technological capabilities.*

White Paper

Demystifying the Capabilities of Quantum Technologies Available Today and in the Future

Chapter 1: Quantum Computing and PQC

ATARC Global Quantum Working Group

Copyright © ATARC 2024

Introduction

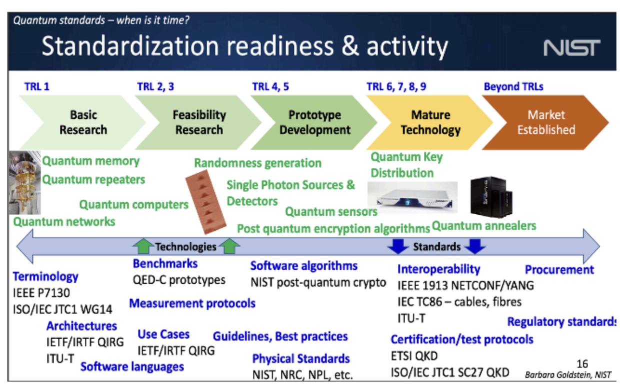
Governments around the world are increasingly engaging with the quantum industry and investing in quantum technologies. The role of the ATARC Global Quantum Working Group is to collaborate with thought leaders within government, academia, and the private sector regarding the multiple aspects of quantum technology. As part of this charge, working group members, which include quantum industry representatives, quantum experts in academia, and government officials involved with quantum programs and/or those who may be end users of the technology, have developed a series of white papers to demystify quantum technology and its capabilities.

Broadly, quantum physics is the "study of matter and energy at the most fundamental level."[1] Quantum technologies exploit quantum physics and quantum mechanical effects which can lead to new capabilities in computing, communications, networking, and sensing. While quantum physics has been studied for decades, it is the newest innovation by the quantum industry which has made tremendous strides in advancing powerful quantum technologies outside the scope of traditional technologies.

Currently, there is no set global standard for technology readiness levels for quantum technologies, so understanding the capabilities of computing, communications, networking, and sensing can be confusing. An overview of the quantum ecosystem and its technologies has been provided by Steve Blank, a U.S. entrepreneur, technologist and professor[2]. That taken in concert with the U.S. National Institute of Standards and Technology's (NIST) baseline for quantum technology readiness[3] (Figure 1) demonstrates that each quantum technology is advancing at its own pace.

To further explain quantum computing, the ATARC Global Quantum Working Group has released two other white papers. "Applied Quantum Computing for Today's Military,"[4] outlined use cases demonstrating how the military could benefit from near-term quantum technology. The second paper was an inter-agency guide on how to be quantum ready and prepare a "Quantum Safe Framework."[5]

Figure 1



[1] https://www.csis.org/analysis/quantum-technology-applications-and-implications
[2] https://steveblank.com/2022/03/22/the-quantum-technology-ecosystem-explained/
[3] https://www.itu.int/en/ITU-T/webinars/20210623/Documents/Goldstein%20Final.pdf?csf=1&e=GdALdj
[4] https://atarc.org/wp-content/uploads/2021/05/ATARC-Military-Paper-by-Quantum-Working-Group.pdf
[5] https://atarc.org/wp-content/uploads/2021/07/Quantum-Safe-Framework-WG-White-Paper_FINAL.pdf

Given the depth of the quantum technology industry, the ATARC Global Quantum Working Group will release chapters of this white paper throughout 2024 focused on different segments of the industry. Chapter 1 will discuss quantum computing and post quantum cryptography (PQC). Future chapters will address quantum sensing, communications, and networking.

Global Government Engagement with Quantum Technologies

Since January 2023, several countries have announced new quantum funding efforts or expansion of their existing quantum programs, including Canada, Australia, Germany, France, India, and the United Kingdom (U.K.). In the U.S., the national quantum strategy falls under the National Quantum Initiative Act (NQI) which Congress was supposed to reauthorize by September 2023. Missing that deadline put the country behind other global leaders on quantum innovation and application development and adoption of current technology.

According to Qureca, as of July 2023, worldwide investments in exploring quantum science and technology totals over $36 billion.[6] (Figure 2). These government quantum programs support funding for all quantum technologies (computing, sensing, communications, and networking), and support initiatives to advance and expand basic quantum research, quantum hardware and software, talent development, and commercialization. Many programs also explicitly support the different quantum computing modalities (annealing, gate, etc.) as well as quantum-classical hybrid technologies[7], which allow quantum and classical computing to work synergistically. For example:

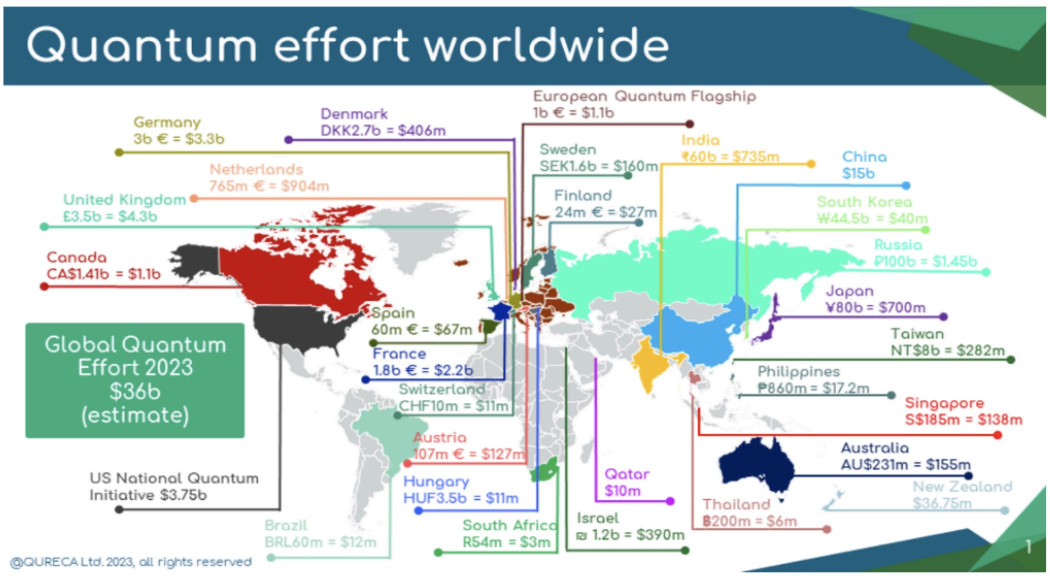
- China has committed to providing $15.3 billion in public funds toward quantum technology and released a new generation of a quantum computing cloud platform that "enables researchers to perform complex computational tasks in the cloud and the public to experience quantum computing at the speed of microseconds."[8]
- The U.K. has announced an application development program which aims to develop quantum applications in an 18-month or less timeframe.[9] Their SparQ program explicitly includes different quantum computing modalities, and in February 2024, the U.K. pledged £45 million to the quantum sector as part of its commitment to transforming to a quantum-enabled economy by 2033.[10]
- Canada released its quantum strategy in January 2023[11] with a three-pillar focus: talent development, research, and commercialization.

[6] https://qureca.com/overview-of-quantum-initiatives-worldwide-2023/
[7] https://www.forbes.com/sites/arthurherman/2022/04/29/the-quantum-revolution-is-here-its-name-is-hybrid/?sh=7289008140fa
[8] https://www.iotworldtoday.com/connectivity/china-launches-its-largest-quantum-cloud-platform
[9] https://iuk.ktn-uk.org/events/quantum-competition-briefings-computing/
[10] https://thequantuminsider.com/2024/02/05/unlocking-the-potential-of-quantum-45-million-investment-to-drive-breakthroughs-in-brain-scanners-navigation-systems-and-quantum-computing/
[11] https://www.canada.ca/en/innovation-science-economic-development/news/2023/01/government-of-canada-launches-national-quantum-strategy-to-create-jobs-and-advance-quantum-technologies.html

- In May 2023, the Australian government released a national quantum strategy and set a $1B funding level.[12]

These are just a few examples, but quantum programs are being developed and/or implemented in other places such as Japan, France, Germany, Ireland, South Korea, India, and the European Union.

Figure 2



***Source:** Overview of Quantum Initiatives Worldwide 2023, @QURECA Ltd. 2023, all rights reserved, July 19, 2023, QURECA News*

U.S. Quantum Policy

The original NQI passed in 2018[13] and created the National Quantum Coordination Office (NQCO), the Quantum Economic Development Consortium (QED-C), and other quantum workstreams across the U.S. government. NQI efforts have also included establishing quantum centers[14] focused on quantum computing, networking, communications, and sensing. Much of the centers' work brings together the national laboratories to address main topics of concern such as noise and fabrication in quantum computing gate-model systems, or new architectures to enhance quantum networking. Congress's failure to reauthorize the NQI by September 2023 has put much of this important work at risk.

[12] https://physicsworld.com/a/australia-sets-out-a1bn-national-quantum-strategy/
[13] https://www.quantum.gov/
[14] https://science.osti.gov/Initiatives/QIS/QIS-Centers

The number of legislative initiatives before Congress demonstrates strong bipartisan support for continuing and expanding U.S. quantum programs. For example, the Quantum User Expansion for Science and Technology (QUEST) program, included in the CHIPS Act[15], helped increase access to commercial quantum computing systems. Funding for QUEST was included in the FY24 Energy and Water Appropriations. While not an exhaustive list of U.S. legislation, these different initiatives demonstrate the broad spectrum of areas that could be addressed by quantum computing.

Much of the quantum policy engagement by Congress expands the focus of the existing NQI programs to enhance engagement of the different quantum technologies, identify use cases, and build near-term applications, supporting talent development, and addressing continuing challenges to hardware advancements.

A sampling of legislation introduced in the 1st session of the 118th Congress includes:

- Reauthorization of the NQI (H.R. 6213)
- Quantum pilot program included in the FY24 National Defense Authorization Act (NDAA), Public Law No: 118-31
- Quantum Sandbox (H.R. 2739, S. 1439)
- Wildfire Tech Demonstration, Evaluation, Modernization, and Optimization (DEMO) Act (H.R. 4235)
- Leveraging Quantum Computing Act (H.R. 3987)
- Quantum in Practice Act (H.R. 1748, S. 969)
- Quantum Computing Cybersecurity Preparedness Act (117th Congress) (H.R.7535)
- Post Quantum Cybersecurity Standards Act (H.R. 5759)
- Quantum Instrumentation for Science and Engineering Act (H.R. 5950)
- Support for Quantum Supply Chains Act (H.R. 6207)
- The GRID Act (S. 3115)

Quantum Computing

Quantum computing represents a paradigm shift in computational capabilities, harnessing quantum mechanics' perplexing yet powerful principles. Unlike classical computers, which process information in binary bits (0s and 1s), quantum computers use quantum bits or qubits. These qubits, leveraging phenomena like superposition and entanglement, can represent both 0 and 1 simultaneously, offering an exponential growth in processing power.

Although quantum computing may be the most well-known of the technologies, there are still misconceptions about the technology's current capability levels. What many don't realize is that quantum computing is not one monolithic technology. Quantum hardware can be comprised of different modalities and the qubits can have different architectures. There are

[15] https://quantumconsortium.org/blog/breaking-down-the-2022-chips-and-science-act/#:~:text=It%20also%20directs%20the%20secretary,years%20for%20the%20QUEST%20program.

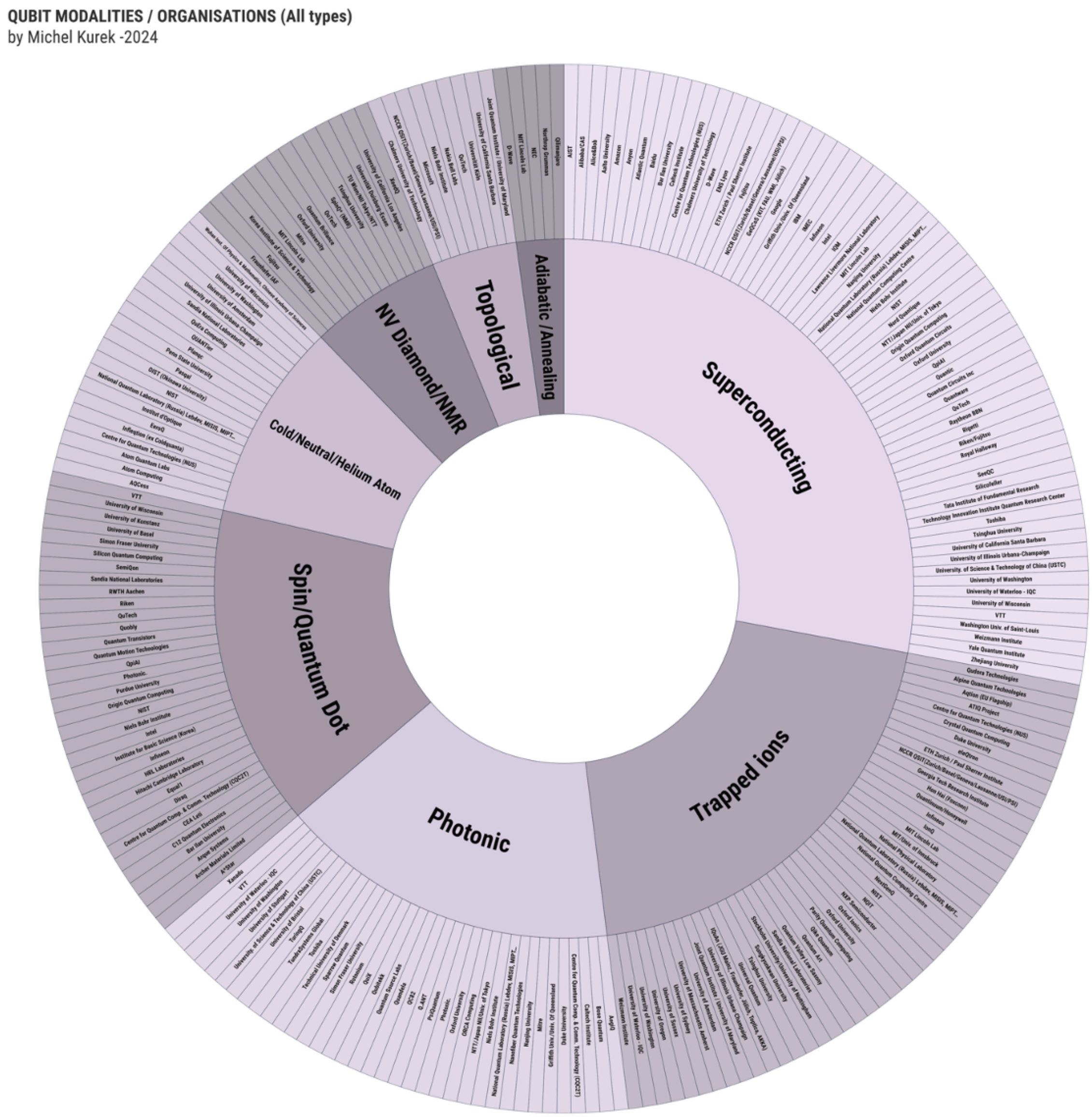
numerous foundational approaches to quantum computing hardware such as gate-model, annealers, topological and others. Brief descriptions are outlined:

- Under gate-model quantum computing, a quantum logic gate is a basic quantum circuit operating on a small number of qubits which become the building blocks of quantum circuits.
- The method for annealing quantum computing (which is a type of adiabatic quantum computation), is to select optimal solutions of problems from a very large number of possible solutions by taking advantage of properties specific to quantum mechanics like: quantum tunneling, entanglement and superposition. Annealing quantum computing harnesses the natural tendency of real-world physical systems to find low energy configurations.
- Topological quantum computing describes the structures that experience physical changes, such as: being bent, twisted, compacted, or stretched; yet the qubit still maintains the properties of the original form.

Beyond the different quantum computing modalities, qubit architecture can range from superconducting, ion traps, neutral spin atoms, photonics, and other technologies.[16] *Figure 3* illustrates the diverse ecosystem of quantum computing modalities which are driving significant progress in the size and robustness of the qubits and providing some error correction methodologies, including innovations from small and large companies, academia, and governments.

[16] https://www.linkedin.com/feed/update/urn:li:activity:7140621985566318593/

Figure 3



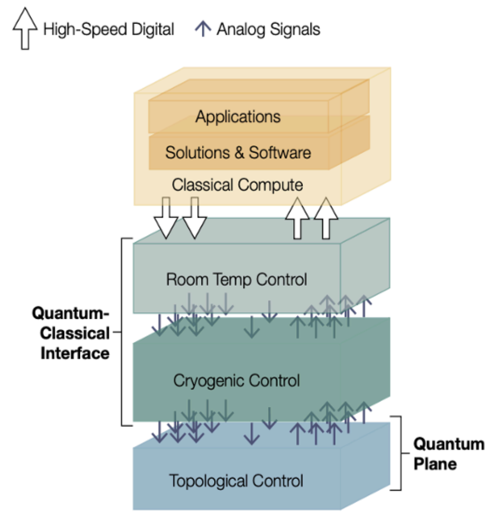
A graphic (*Figure 4*) from the Hudson Institute report, "*Advancing the Quantum Advantage: Hybrid Quantum Systems and the Future of American High-Tech Leadership*"[17] illustrates how hardware and software work together in quantum computing. Development of quantum-classical hybrid technologies have flourished over the past few years.

---

[17] https://www.hudson.org/innovation/advancing-quantum-advantage-hybrid-quantum-systems-future-american-high-tech-leadership

Many quantum computers today are cloud accessible through a variety of different platforms including AWS Braket and AWS Marketplace, Microsoft Azure, and Google Cloud, and company operated or Open-Source platforms like IBM's Qiskit, D-Wave's Leap™ quantum cloud service, or Quantinuum's TKET. Cloud access has provided broader access for a more diverse set of researchers and organizations to build applications utilizing these powerful computational technologies. These advancements, along with quantum-classical hybrid computing technologies, enable quantum computing to tackle many practical public-sector problems such as emergency response, supply chain challenges, electric grid resilience, and securing network communications.

Figure 4



Source: Chetan Nayak, "Full Stack Ahead: Pioneering Quantum Hardware Allows for Controlling up to Thousands of Qubits at Cryogenic Temperatures," Microsoft Research Blog, January 27, 2021, https://www.microsoft.com/en-us/research/blog/full-stack-ahead-pioneering-quantum-hardware-allows-for-controlling-up-to-thousands-of-qubits-at-cryogenic-temperatures/.

Quantum Application Software

There are parallels between the evolution of quantum computers that are available today and classical computer hardware and software. Each step in the evolution of classical computer software has made it easier for organizations and individuals to focus on their mission and not what was "under the hood" in the cloud data center or in the chipsets on their laptop or smartphone.

In classical computing, first came assembly languages that were tied to a specific hardware. Later came portable languages could run on any machine, making programming and scaling of usage easier. Development of application software like ERP, word processing, and spreadsheets created the killer apps that drove the classical industry. In the quantum realm, the software applications currently being developed will leverage the strengths of quantum computers to work synergistically with other technologies e.g. classical computing, AI, and machine learning. While the world waits for the "killer app", quantum computing technology that is available today is already addressing public-sector problems, especially when incorporating quantum-classical hybrid applications.

As highlighted by Deloitte[18], government can be a first user of quantum computing technology by building applications to tackle public-sector challenges. Public-sector use cases related to areas such as emergency response[19] and sustainability, have already provided benefit. To help address global supply chain strain, the Port of Los Angeles[20] used quantum computing to optimize a cargo pier. As a result, the quantum application increased truck turnaround time by

[18] https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-quantum-technology-public-sector.html

[19] https://federalnewsnetwork.com/commentary/2023/07/emergency-management-today-quantum-computing-is-a-21st-century-solution-for-21st-century-problems/

[20] https://nam.org/how-quantum-computing-reorganized-a-pier-22712/

12% and the movement of 60% more cargo. Additionally, the Australian government has announced their intentions to use quantum computing applications to optimize its transportation systems,[21] and in Europe, the 2023 myEU Space program[22] highlighted quantum-hybrid applications to explore low earth satellite observations.

As many government quantum programs expand their focus to include both near-term applications and longer-term hardware advancements, these programs must be inclusive of the different modalities and qubit architectures. Due to this expanded timeline focus, this white paper will provide insight into the types of problems that can be solved in the near-term (1-3 years), mid-term (3-7 years) and long-term (7+ years). Many scientific hurdles must still be addressed through fundamental scientific engagement, such as increased coherence timing and error mitigation. For the purposes of this white paper, we will not delve deeply into these topics. Since the timeline for achieving these scientific hurdles are uncertain, the mid-term and long-term application timing may shift based upon achieving the needed advancement of quantum hardware.

While this white paper is not intended to be a comprehensive list of problem sets, it will provide a high-level overview of the types of challenges that quantum computing and quantum-classical hybrid applications can address across different timelines and a guide to the "art of the possible" for future generations of quantum computing systems and software.

Quantum Computing: Near-Term Applications (1-3 years)

Today's quantum technology, while still nascent, can provide solutions to a variety of problems. By harnessing the power of quantum algorithms, businesses and governments can tackle complex problems. With cloud access to quantum computing technology, and advancement of quantum-classical software applications, some problems are within reach of providing better, or perhaps faster, solutions with quantum computing technology that is available today.

Optimization

Many problems, both in the public and private sectors, can benefit from optimization which can be found in logistics, manufacturing, staff scheduling, emergency response, military, and in many other areas. Today's quantum computing technology may provide solutions which are better than using classical computation alone. According to McKinsey[23], quantum optimizers can deliver benefits for solving optimization problems across industries, in weather forecasting, and materials science. For example:

- The Defense Advanced Research Projects Agency (DARPA) called for application development utilizing quantum computing technology in their Imaging Practical

[21] https://www.transport.nsw.gov.au/system/files/media/documents/2021/Transport%20for%20NSW%20and%20Quantum%20Technology%20-%20WCAG%20version.PDF
[22] https://thequantuminsider.com/2023/06/17/2355920/
[23] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/early-value-an-introduction-to-quantum-optimizers

Applications for a Quantum Tomorrow (IMPAQT)[24] program. Similar calls have occurred in the U.K.[25] through their quantum application feasibility program.

- In the U.S., the QED-C identified problems in the energy and utility space which can be addressed with today's technology such as electrical grid resilience[26] and electrical grid security.[27] Some of use cases described in the quantum consortium's grid security paper have longer timelines and will likely fall into the mid-term timeframe.
- A European energy company, Vinci Energies,[28] is developing quantum computing applications to optimize heating, ventilation, and air conditioning (HVAC) in construction projects. In Japan, an application optimized construction site operations by 10%.[29] At the local and state level, governments could develop applications for infrastructure projects such as housing, that optimize the construction site and HVAC within those units.
- Environmental efforts could also benefit from optimization. For example, many government initiatives are addressing concerns about PFAS, commonly called forever chemicals, which have an impact on human and animal health and the environment.[30] While some parts of the PFAS problem, such as optimizing clean-up and remediation efforts, are within the scope of today's quantum technologies,[31] other parts like new chemical design and chemical simulation will have a longer timeline and would likely fall under the long-term timeframe.
- Another area that could benefit from today's quantum computing is lowering CO2 emissions. In the U.S., the Net Zero World Initiative[32] leverages expertise across U.S. government agencies and U.S. Department of Energy national laboratories for a whole-of-government approach focused on advancing decarbonization. While large-scale weather modeling and global forecasting is outside the scope of near-term applications, applications have reduced CO2 emissions through optimized waste collection routing in Japan.[33]

As this white paper has demonstrated, many public sector problems could benefit from optimization applications utilizing the computational power of quantum-classical hybrid technologies.

---

[24] https://www.darpa.mil/research/programs/impaqt
[25] https://apply-for-innovation-funding.service.gov.uk/competition/1468/overview/3e95c2d9-70ba-4a06-880f-c814422bb1f1
[26] https://quantumconsortium.org/QUEnergy22/
[27] https://quantumconsortium.org/quenergy23/
[28] https://www.businesswire.com/news/home/20231219235223/en/International-Collaboration-between-VINCI-Energies-QuantumBasel-and-D-Wave-Improves-Efficiency-in-HVAC-System-Design-with-Quantum-Computing
[29] https://www.dwavesys.com/media/c2bhs1o1/dwave_groovenauts_case_story-2_v5.pdf
[30] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/14/fact-sheet-biden-harris-administration-takes-new-action-to-protect-communities-from-pfas-pollution/
[31] https://nam.org/how-quantum-computing-can-combat-forever-chemicals-29001/
[32] https://www.nrel.gov/international/net-zero-world.html#:~:text=The%20Net%20Zero%20World%20Initiative,energy%20systems%20for%20our%20partners
[33] https://www.magellanic-clouds.com/blocks/en/2020/03/30/mec/

Simulations and Modeling

As discussed in the ATARC white paper, *Applied Quantum for Today's Military*, battlefield simulations are an integral part of military training, and cloud computing has provided the infrastructure to migrate an entire simulation environment to a virtual environment. Quantum computers, along with virtual reality, augmented reality, mixed reality, AI, and machine learning capabilities will be critical for mission preparedness. Currently, many simulations for a mission must be performed and combined with situational awareness intelligence to provide a more complete response. The goal is for a decision to be based on situational awareness and simulated possible situation evolution. Applied quantum computing, which can be enriched by quantum-enhanced AI, could be utilized by defense architects for mission-scale simulations of military deployments, and other scenarios, to provide real-time or near real time analysis to commanders.

Beyond military applications, quantum simulations are also important in medical discovery. According to the University of Waterloo,[34] many diseases have one thing in common; they are caused by misfolded protein molecules. Quantum simulations can help understand protein folding which may ultimately help cure some diseases.

Machine Learning and AI

Machine learning can take advantage of quantum computing by unlocking the computational power needed to build massive AI models from large datasets. Research detailed in a recent Nature article,[35] suggests quantum machine learning and AI can achieve exponential speedups. A comprehensive review article[36] on quantum machine learning identifies up to 18 machine learning algorithms suitable for quantum advantage, encompassing applications such as quantum support vector machines, Boltzmann machines, and Quantum Neural Networks. These diverse algorithms showcase their potential applications in critical domains like material and drug discovery, precision medicine, finance, and more.

The private sector is at the forefront of initiatives to harness the synergy between AI and quantum computing. For example, SanboxAQ, a spin-off of Google, has recently intensified its commitment to quantum computing for expediting AI-based drug discovery.[37] Moreover, companies such as IBM[38] and PASQAL[39] are actively involved in the development of quantum generative models. NVIDIA has partnered with Qubrid to build quantum machine learning applications, leveraging their hybrid classical-quantum platform and quantum software libraries.[40] D-Wave and Zapata AI have also begun work on quantum and AI for molecular

---

[34] https://uwaterloo.ca/institute-for-quantum-computing/quantum-101/quantum-information-science-and-technology/quantum-simulation
[35] https://doi.org/10.1038/s42256-023-00710-9
[36] https://doi.org/10.48550/arXiv.2201.04093
[37] https://www.hpcwire.com/off-the-wire/sandboxaq-acquires-good-chemistry-to-accelerate-ai-simulation-platform-for-drug-discovery-and-material-science/
[38] https://www.ibm.com/case-studies/cern/
[39] https://www.hpcwire.com/off-the-wire/pasqal-partners-with-mila-to-enhance-generative-modeling-in-quantum-ai/
[40] https://www.insidequantumtechnology.com/news-archive/qubrid-aligns-with-nvidia-integrates-cuquantum-cuda-quantum/

discovery.[41] These concerted efforts underscore the growing integration of quantum computing into the landscape of AI and machine learning.

Drug Discovery

As highlighted in the quantum and machine learning section above, there are parts of drug discovery that could benefit from today's quantum technology. While quantum chemistry and personalized medicine are likely in the long-term timeframe, there are parts of drug discovery which can benefit from today's quantum technology. Drug maker GlaxoSmithKline assessed using quantum computing to address mRNA codon optimization[42] which is important for downstream processes such as protein folding, a function used in recombinant protein therapies. PolarisQB, a U.S. based start-up is exploring how quantum computing can assist with new drugs and they received a DARPA grant for "Quantum Computing Solutions for Inhibiting Protein-Protein Interactions for Emerging Threats." The objective of the project is to make a novel variational quantum algorithm (VQA) that identifies small molecules that inhibit protein-protein interactions, one of the most challenging areas of drug design. [43]

Cybersecurity Leveraged from a Quantum Computer

One of the first scaled production uses of a quantum computer is generating and proving entropy (randomness)[44] which is required to generate strong keys to support robust classical cryptography (RSA, ECC, AES) and the new NIST FIPS candidate PQC algorithms (Kyber, Dilithium, Spincs+), key management and distribution. This capability has been added to the software in certified tools such as Thales HSM[45] which underpins global banking infrastructure, Fornetix ICAM[46] that secures government communications, and in Honeywell's IIoT meters[47] across the world.

Adversaries initially try to break into sensitive data through "Store Now Decrypt Later" attacks where a nefarious actor will harvest encrypted data and hold it until they are able to later decrypt it. Historically, cryptographic systems in end points, cloud infrastructure, and networks appliances had to rely on pseudo random number generation in software, randomness from a local CPU, or try to bolt-on new hardware to generate keys, none of which were provably random and easy to scale in software defined architectures.

With global investment in higher education, high performance computing, and quantum computing improving capabilities across the board, we can no longer believe that "nobody but us" will be able to crack keys generated from weak entropy, or algorithms using 1970s Public

[41] https://www.dwavesys.com/company/newsroom/press-release/d-wave-and-zapata-ai-announce-strategic-technical-and-commercial-collaboration-to-advance-quantum-enabled-machine-learning/
[42] https://www.nextplatform.com/2021/02/24/glaxosmithkline-marks-quantum-progress-with-d-wave/
[43] https://polarisqb.com/blog/polarisqb-receives-darpa-impaqt-funding-to-advance-quantum-computing-for-drug-design/
[44] https://arxiv.org/abs/2009.06551
[45] https://cpl.thalesgroup.com/blog/data-protection/build-quantum-resilience-thales-quantinuum
[46] https://www.fornetix.com/wp-content/uploads/2017/05/fornetix-press-release-thales-rsa-2017.pdf
[47] https://www.honeywell.com/us/en/press/2023/09/honeywell-leverages-quantum-computing-encryption-keys-to-bolster-utilities-data-security-against-cyber-threats

Key Infrastructure (PKI). Weak cybersecurity facilitates nation state surveillance, opens the door for denial-of-service attacks by criminals, and can lead to property damage, injury, and potentially death if the integrity of supervisory control and data acquisition systems is compromised by cyber weapons.

Quantum Computing: Mid-Term Applications (3-7 years)

As quantum computing hardware and software continue to advance and overcome some of the limitations of today's systems due to noise errors, other problem sets may be tackled with these larger, more coherent, systems. As mentioned above, some of these timelines may shift based upon achievements of scientific advancements in hardware.

New Material Design

While the timeline is not fully realized, it is anticipated that quantum computing could help manufacturers better understand how to incorporate new materials into products, such as batteries. According to Tech Target[48], quantum computing could provide more insight into how to optimize batteries for longevity and efficiency and gain a better understanding of lithium compounds and battery chemistry. Some in the industry are looking at quantum computing for PFAS chemistry simulations which may fall into the mid-term or even long-term timelines.[49]

Scientists at Ames Laboratory[50], a Department of Energy national lab, are working to harness the power of quantum computers with adaptive algorithms for simulating new material. A primary research focus at Ames Lab is rare earth materials which are used in a variety of technology, including smart phones, computer hard drives, light-emitting-diodes (LEDs), electronic displays, and permanent magnets for alternative energy technology, such as wind turbines. Additional research is being conducted within industry such as OTI Lumionics[51] who is exploring how to solve problems facing displays and lighting.

Finding alternative materials that can substitute rare earths for less expensive and more available materials can be focus for more mature quantum computing technology. According to Boston Consulting Group, quantum computing technology, when more mature, can develop more efficient chemical catalysts, and eventually be used to develop lighter and stronger materials for building cars and aircraft.[52]

Weather Modeling and Forecasting[53]

While some small-scale weather modeling can occur with today's quantum technologies, as hardware systems advance, improved weather forecasting should be within scope. Today's

[48] https://www.techtarget.com/searchdatacenter/tip/Explore-future-potential-quantum-computing-uses
[49] https://arxiv.org/abs/2311.01242
[50] https://www.ameslab.gov/news/scientists-take-an-important-step-towards-using-quantum-computers-to-advance-materials-science
[51] https://www.dwavesys.com/media/ghhnqkuv/18_oti_qubits_march2019.pdf
[52] https://www.bcg.com/capabilities/digital-technology-data/emerging-technologies/quantum-computing
[53] https://arxiv.org/abs/2210.17460

classical computers cannot process the vast amounts of details that impact weather, and their limitations are apparent as the time to solution is too long to provide actionable information in a timely manner. Scientists believe that the ability for quantum technologies to analyze vast amounts of data at once will provide more accurate and quicker predictions such as improving warnings for natural disasters. Some applications are already being built today to address emergency response through low earth orbit satellite optimization. Moreover, the University of Toronto in Canada is exploring how quantum computing can be used to improve global climate models. However, larger-scale forecasting will need larger, more coherent, systems which are still a few years away.

Figure 5

Staffing and Timeline for Contingency Analysis for Resilience

Contingency Analysis for Resilience						
Project	**Contingency Analysis**					
Goals	Speed, scalability, better convergence, improved resilience					
Timeline	2m	4m	6m	8m	10m	12m
Activities	Problem definition & design	Data rationalization & acquisition	Research, design, experiment & infrastructure, runtime			Publish & deploy
Project	**Optimization for Resilience**					
Goals	Compare against classical optimization: response time, explored problem space. Grid statistics: uptime, efficiency, system stability (blackouts / brownouts), power quality (cascading power failures)					
Timeline	1yr	2yr	3yr	4yr	5yr	6yr
Activities	Educate & collaborate	Research	Solve	Develop		
Project	**Planning Optimization: Distribution Grid with EV integration, Transmission Expansion, Generation Expansion**					
Goals	Sustainable energy production, reduced environmental impact, increase flexibility, increased resilience					
Timeline	2yr	4yr	6yr	8yr	10yr	12yr
Activities	Gather data sources and test algorithms on quantum devices (Feasibility)	Scalability to larger sized optimization and simulation problems (Scalability)		Planning used for real-world power grid use cases (Demonstration)		

Electrical Grid Security

While electrical grid resilience may have some applications in the near-term, much of the grid security efforts will need more advanced quantum computers. For example, electrical grid contingency analysis, which allows for more accurately identifying vulnerabilities, can benefit from today's quantum computing systems. However, according to the QED-C QuEnergy report for grid security,[54] long-range planning, transmission and infrastructure analysis, and deployment will fall in longer timeframes. *Figure 5* illustrates the variety of different examples identified by QED-C which can fall across the different timelines.

Quantum Computing: Long-term use cases (7+ years)

Perhaps the most discussed topic related to quantum computing technology is that it could one day break encryption. In reality, Q-Day, the day a quantum computer is big enough to break encryption, is many years away, and the actual timeline is still under debate. Scientists predict that as the hardware grows in scale, longer-term applications will include cryptography along with quantum chemistry advancements, including personalized medicines and new materials.

[54] https://quantumconsortium.org/quenergy23/

To recap, the timelines are less predictable for the longer-term use cases as scientific advancements in hardware are needed, and scientific hurdles must be overcome to reach error-corrected and larger quantum computing systems.

Challenges for Quantum Computing

Quantum computing has made important advancements as systems are now available via the cloud and quantum-classical hybrid applications are tackling real-world problems, however, challenges remain for quantum computing technology's continued advancement.

- **Hardware:** Quantum computing companies must still address error correction, coherence of qubits, and scalability. The timeline for achieving these advancements may vary for the different quantum computing modalities and qubit architectures. New and larger systems are being released at a rapid pace, but better coherence times and error correction are needed to ensure future scalability of quantum computing systems. As advancements and research in the hardware continues into the foreseeable future, government programs should continue to fund this research and be inclusive of the various quantum computing modalities and qubit architectures within their programs.
- **Software:** Due to the fact that quantum-classical hybrid algorithm development has only begun in the past few years, innovations and increased focus on the software layer of quantum computing will be critical in the coming years. Advancements in the software stack and cloud access to systems have created an environment for the emergence of new companies building quantum-classical hybrid applications. Many of these start-ups focus on specific problems sets or industries. Since this field is still emerging and new innovations are occurring rapidly, additional quantum-classical interfaces may be needed to help boost quantum-hybrid technology advancements. Therefore, U.S. government quantum programs must expand to include a new area of focus within quantum-classical hybrid application development.
- **Infrastructure:** There are calls for integrated development of data centers which co-locate both classical and quantum computers. According to data center expert Paul Bevan of Bloor Research, while quantum computers are primarily found in supercomputing centers and national labs, there will be a gradual integration with mainstream data centers.[55] Infrastructure projects integrating quantum computing into data centers is necessary to continue addressing future needs of end-users and must be included in U.S. government infrastructure projects. These data centers should focus on inclusivity of the different quantum computing modalities and qubit architectures as each type of system may provide different strengths for diverse problem sets.

[55] https://techmonitor.ai/hardware/quantum/data-centre-quantum-computer

- **Talent:** Talent is a challenge for quantum computing companies and end users, including government. The Government Accounting Office released a report[56] discussing the need for talent within the Department of Defense (DoD) and the inconsistencies with workforce planning. Within the DoD structure, there is also a lack of knowledge and engagement with the different types of quantum computing systems and software layer of the technology which must be addressed through training programs and broader engagement with the quantum computing industry. Talent development is a key focus for nearly all government quantum programs including the NQI in the U.S. The government should tap into the private sector's training programs to upskill its workforce to better understand the capabilities of today's quantum technology, especially as it relates to algorithm development and how quantum can work in concert with other technologies such as zero trust, AI, and machine learning.

Once these hurdles are addressed and scientific advancements have been achieved, timelines for mid-term and long-term use cases will become more clearly defined.

Post Quantum Cryptography

The quantum leap that has been discussed in this paper is not without repercussions, particularly in the realm of cryptography which is critical to securing digital information and communications in the modern world. Its primary function is to protect sensitive data from unauthorized access and ensure its integrity during transmission by converting plain text into an unreadable format (encryption) and then back into its original format (decryption) by authorized parties. Cryptography ensures that the data remains confidential and secure from interception or tampering by external entities. It also verifies the authenticity of the sender and receiver, thus preventing impersonation and unauthorized access, and maintains data integrity, ensuring the information has not been altered during transmission. The role of cryptography is vital in various domains, including securing communication, protecting personal identifiable information (PII), and safeguarding intellectual property in the digital age.

Modern cryptographic algorithms, the bedrock of digital security, rely heavily on the computational difficulty of certain mathematical problems, like factoring large numbers, a task that quantum computers could perform exceedingly fast. However, quantum computing could break widely used cryptographic algorithms such as RSA and ECC, which secure everything from email communications to financial transactions.

While the timeline for developing quantum computers capable of breaking current encryption is still an active topic of debate, the consensus among experts is that it's not a question of "if" but "when," and therefore governments and businesses must begin their identification of sensitive data in the near-term. The most immediate threat, as discussed above, is the "Store

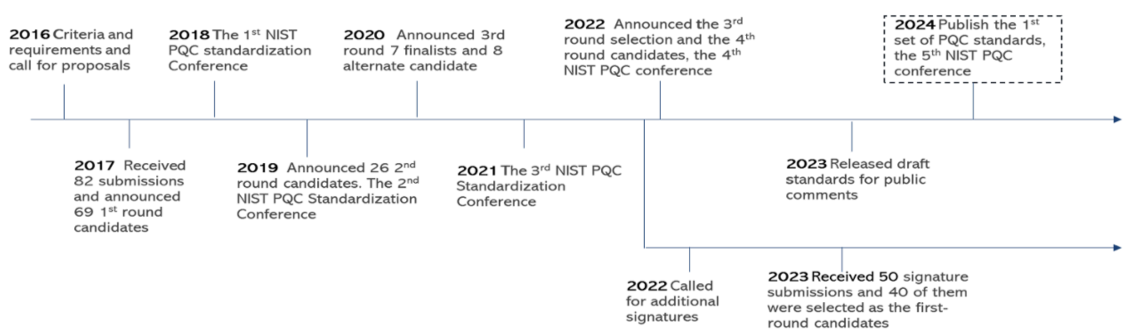
[56] https://www.gao.gov/products/gao-24-106284

Now and Decrypt Later" where adversaries are storing encrypted data now and waiting for development of a large-scale error corrected quantum computer that can break encryption and gain access to sensitive information. This poses a serious and current risk to the stored data's confidentiality, availability, and integrity, potentially leading to unauthorized access, data breaches, and compromised security. The risk is significant enough to warrant proactive measures to adopt and migrate to quantum-resistant encryption methods, ensuring the security of sensitive data in the quantum computing era. To avoid the potential catastrophic impact of quantum computers to cybersecurity, it has been an urgent task to standardize new cryptographic algorithms which can resist quantum attacks. This class of algorithms are called post-quantum cryptography (PQC).

PQC and U.S. Government Activities

PQC is an active research area. To resist quantum attacks, the security of algorithms must be based on hard problems which are both hard for classic computers and quantum computers. Many literatures have provided comprehensive surveys regarding categories of post-quantum cryptography[57,58].

Figure 6



To deploy PQC to real-life cybersecurity applications, the first step is developing standards. As outlined in *Figure 6*, NIST initiated a process in 2016 through a public call for proposals with requirements and criteria for post-quantum cryptography algorithms which resulted in 82 submissions with researchers from 25 countries.[59] The submitted algorithms were analyzed and evaluated by the research community for their security and performance for cybersecurity applications. By 2022, NIST has narrowed the candidate pool twice and selected four algorithms to be standardized. At the time of this white paper, NIST has published the first set

[57] https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf
[58] https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
[59] https://csrc.nist.gov/projects/post-quantum-cryptography

of three Federal Information Process Standards (FIPS)specifying three of the four selected algorithms. One FIPS specifying another selected algorithm is under development. As NIST continues the effort to develop additional PQC standards, including selection on the 4 th round candidates and evaluation on the additional signature candidates, NIST released draft NISTIR 8547 "Transition to Post-Quantum Cryptography Standards"[60] in November 2024. It identifies existing quantum-vulnerable cryptographic standards and the quantum-resistant standards to which information technology products and services will need to transition.

Migration to PQC is going to be an extremely challenging task because quantum-vulnerable cryptographic algorithms have been implemented in almost all digital devices we use today, including servers, Internet routers, desktop computers, laptops, and cell phones. The National Security Memorandum 10 released on May 4, 2022[61] directs NIST to establish a "Migration to Post-Quantum Cryptography Project" at the National Cybersecurity Center of Excellence (NCCoE), and an open working group with industry to generate research on, and encourage widespread, equitable adoption of, quantum-resilient cryptographic standards and technologies. NCCoE has initiated a collaboration platform with industry partners to approach migration strategies and develop technologies, including creating white papers, playbooks, and proof-of-concept implementations.[62] A series of NIST Special Publications 1800-38s is under development and a draft has been released for public comment.[63]

While quantum computing brings incredible benefits to science and technology, the impact to cybersecurity is concerning. In the quantum era, PQC is intended to be the new tool for cybersecurity.

Successful Migration to PQC: Necessary Steps for Organizations

As the threat of quantum computing looms, organizations must take proactive steps to ensure the security of their cryptographic systems such as deploying cryptographic agility to respond at the speed of the changing threat landscape. The following steps, based on guidance provided by the Cybersecurity and Infrastructure Security Agency, National Security Agency, and NIST, can help organizations successfully migrate to PQC:

Establish a Quantum-Readiness Roadmap

- Develop a roadmap outlining the organization's strategy and timeline for transitioning to PQC.
- Identify key milestones, resource requirements, and potential challenges.
- Ensure alignment with industry standards and best practices.

Prepare a Cryptographic Inventory

[60] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
[61] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[62] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
[63] https://content.govdelivery.com/accounts/USNIST/bulletins/38000a3

- Conduct a comprehensive assessment of the organization's cryptographic systems and algorithms.
- Identify the current encryption algorithms and their vulnerability to quantum attacks.
- Prioritize systems and applications based on their criticality and potential impact.

Understand and Assess Supply Chain

- Evaluate the organization's supply chain to identify dependencies on cryptographic systems and algorithms.
- Assess the potential risks associated with quantum-vulnerable cryptography in systems and assets.
- Engage with suppliers and vendors to understand their plans for PQC adoption and ensure compatibility.

Engage with Technology Vendors

- Establish communication channels with technology vendors to discuss PQC and their plans for implementing quantum-resistant solutions.
- Seek information on the availability of PQC-compatible products and services.
- Collaborate with vendors to ensure a smooth transition to PQC without compromising security.

Assess Quantum Risk

- Conduct a thorough risk assessment to understand the potential impact of quantum computing on the organization's cryptographic systems.
- Evaluate quantum attacks' likelihood and potential consequences on current encryption methods.
- Use the assessment to inform decision-making and prioritize migration efforts.

Stay Informed and Engage with Industry

- Stay updated on the latest developments in PQC standards and research.
- Engage with industry forums, conferences, and working groups to share knowledge and best practices.
- Collaborate with peers and experts to gain insights into successful migration strategies.

As the PQC field continues to evolve, it is essential to stay informed, collaborate with industry stakeholders, and adapt strategies.

Chapter 1: Conclusion

Quantum computing technology provides great benefits today and in the future. Understanding the technology readiness level and engaging holistically with the technology is critical to ensuring U.S. leadership in quantum innovation. Programs must be aimed at hardware advancements and software development that is inclusive of the different computing modalities and qubit architectures.

Balancing the near-term benefits with long-term advancements is key to advancing quantum Policy makers are engaging with the quantum industry in a new way, including expanding U.S. quantum programs to include near-term and mid-term use cases. The first step is for end users of the technology, both in the public and private sector, to understand problems facing their industry or agency and identify those that could benefit from quantum computing technologies. While use case identification is occurring around the globe, the quantum sandbox and testbed programs in the U.S. are not actively engaged in application development compared to other governments. Meanwhile, organizations like QED-C, the Mitchell Institute,[64] and the Center for Data Innovation[65] are highlighting potential areas where today's quantum computing technology can provide some benefit, mirroring Congressional intent for bipartisan quantum legislation.

For PQC, addressing the needs of government will take a whole-of-government approach and an agile mindset. The White House readout[66] from a roundtable discussion outlined the NSM-10 requirements on *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems* and the *Quantum Computing Cybersecurity Preparedness Act of 2022*. It is imperative that government engage with industry to ensure U.S. cyber defenses remain resilient and nimble so they can respond at rapid pace to a changing threat landscape. Organizations and the government must prepare in advance and be ready to migrate to PQC algorithms prior to the eventual existence of a large-scale error corrected quantum computer. As NIST identifies and promotes strong encryption standards and methodologies, agencies and those who support the public sector must begin migration.

As quantum computing systems continue to advance, the technology will be able to address new and larger problem sets. But waiting for Q-Day is not necessary to benefit from today's technology. There are a host of problems for which quantum computing and quantum-classical hybrid technologies can address and, in some cases, provide solutions which are better and/or faster than classical computation alone. Finally, as the government prioritizes the acquisition and migration of federal agencies' information technology to PQC, the work impacting agencies and government contractors must begin immediately even though the threat may be years away.

---

64 https://mitchellaerospacepower.org/the-quantum-advantage-why-it-matters-and-essential-next-steps/

65 https://itif.org/publications/2021/04/27/why-united-states-needs-support-near-term-quantum-computing-applications/

66 https://www.whitehouse.gov/omb/briefing-room/2024/02/12/readout-of-white-house-roundtable-on-protecting-our-nations-data-and-networks-from-future-cybersecurity-threats/

White Paper

Demystifying the Capabilities of Quantum Technologies Available Today and in the Future

Chapter 2: Quantum Sensing

ATARC Global Quantum Working Group

Copyright © ATARC 2024

Quantum Sensing

The quantum revolution consists of a surge in quantum technology development capable of disrupting numerous industries. Quantum sensing is one such technology. Quantum sensing is an advanced sensor technology that aims to vastly improve the "accuracy of how we measure, navigate, study, explore, see, and interact with the world around us by sensing changes in motion, and electric and magnetic fields. The analyzed data is collected at the atomic level."[67] By collecting data at the atomic level, quantum sensing technology more accurately detects variations in motion, as well as electric and magnetic fields. This enhances our ability to measure, study, and understand our surroundings.

While realizing the full potential of many quantum technologies may still be years away, tech development is rapidly progressing, promising to unlock new capabilities across various applications and industries. For quantum sensing, the technology is viewed to be more mature than other quantum technologies, and this chapter aims to provide a non-technical review of quantum sensing technologies and discuss their capabilities and maturity levels.

Quantum Sensing and Metrology

Quantum properties can be used to significantly enhance sensing and measurement techniques, enabling precision measurements beyond what is possible with classical physics alone. According to Jonathan Dowling, a former U.S. professor in theoretical physics who specialized in quantum sensing and quantum imaging, and Gerard Milburn, an Australian theoretical quantum physicist who specialized in quantum feedback control and quantum measurements, the impact of quantum sensing on fields such as navigation, radiofrequency communications, geological surveying, and medical diagnostics will be significant. Their research shows quantum sensing will provide more accurate and sensitive detection of environmental changes, gravitational fields, electromagnetic radiation, and even molecular structures.[68] Since quantum sensors rely on quantum particles to make measurements, they are inherently more sensitive than traditional sensors, which introduces a significant range of new applications, data insights, and decision-making capabilities.

Global Interest in Quantum Sensing

As with all quantum technologies, there is interest across governments to advance the science, build the industry, and expedite adoption of powerful quantum sensing technologies. NQI funds research projects, workforce development, and public-private partnerships and the

---

[67] https://www.baesystems.com/en-us/definition/what-is-quantum-sensing#:~:text=Quantum%20Sensing%20is%20an%20advanced,collected%20at%20the%20atomic%20level

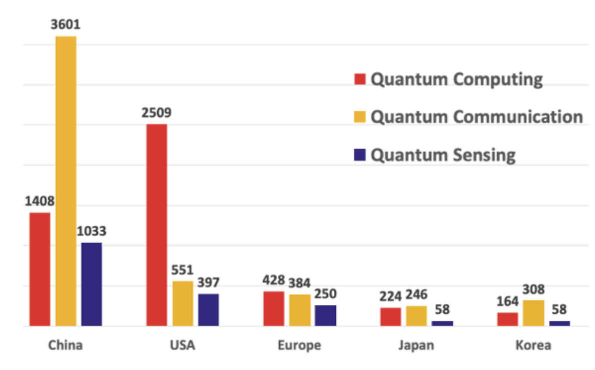
[68] https://royalsocietypublishing.org/doi/10.1098/rsta.2003.1227

quantum sensing programs are focused on accelerating the development of new approaches and prioritize appropriate partnerships with end users to elevate the technology readiness of new quantum sensors. The U.S. government is interested in quantum sensing applications for national security, including threat detection and secure communication, as well as healthcare for early disease detection. However, use of quantum sensing technology is much broader and can impact a variety of different industries including telecommunications, manufacturing, oil & gas, and more. According to the U.S. National Science & Technology Council[69], the realization of new quantum sensors is tangible, and therefore, a near-term objective should be to enhance adoption of quantum sensors as it will provide a foundation for providing disruptive advantages in a variety of different applications.

The European Union's (E.U.) Quantum Flagship Initiative aims to solidify Europe's position in the global race for quantum technologies including dedicated research projects on quantum sensing, focusing on areas like magnetometry and gyroscopes.[70] The E.U. is particularly interested in quantum sensing applications for navigation, including enhanced GPS capabilities, environmental monitoring, and fundamental science research.

In China, the National Key R&D Program identifies quantum technologies as a strategic priority, listing quantum sensing as a key focus area. Significant investments in that region are being made in research institutions and government-backed companies developing quantum sensing technologies. China is interested in applying quantum sensing technology to advance national security and resource exploration (oil & gas).

Figure 1: Quantum Patents by Country

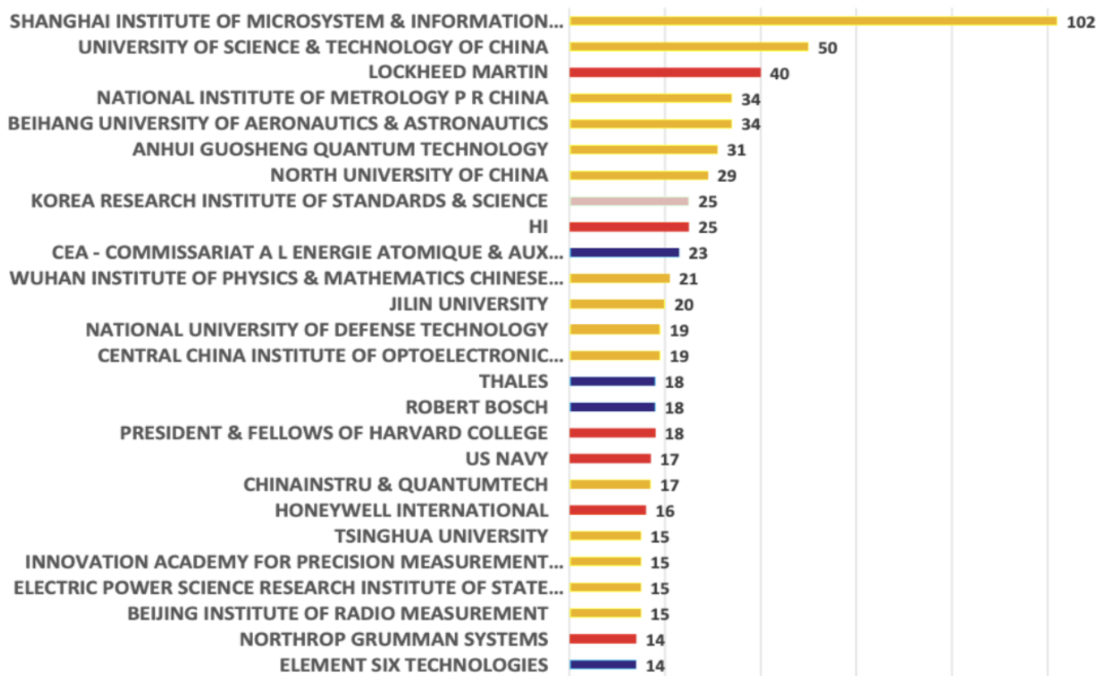


The vast number of quantum patents issued across the globe represents the widespread interest in quantum sensing technologies (see Figure 1). In their 2024 review of quantum patents by country, the European Quantum Consortium (QuIC)[71] showed China leading the way with quantum communications and quantum sensing patents, while the U.S. has the largest number of quantum computing patents.

According to QuIC, the patents for quantum sensing (see Figure 2) show the companies, academia and areas of the globe which are heavily focused on quantum sensing technologies. Most of the Chinese patents are with academia while other global regions patents are held by industry and government.

[69] https://www.quantum.gov/wp-content/uploads/2022/03/BringingQuantumSensorstoFruition.pdf
[70] https://qt.eu/projects/index
[71] https://www.euroquic.org/wp-content/uploads/2024/03/QuIC-White-Paper-IPT-January-2024.pdf

Figure 2: Quantum Sensing Patents by Patent Family



Interest is not solely within governments. According to a recent report from Citi Global Insights, in 2023, venture capital invested $80 million in quantum sensing companies. Citi Global Insights believed that a market of $3.25-5bn could develop for just one type of quantum sensor, in the aviation industry alone.[72]

Understanding Quantum Sensing

Traditional sensor technologies face several limitations that hinder a sensors ability to measure certain phenomena with the utmost detail. Those limitations include:

- **Sensitivity:** Traditional sensors can only detect signals above a certain threshold. Weak signals, which are crucial for early disease detection or faint environmental changes, often fall below this threshold and remain undetected by traditional sensors.
- **Precision:** All sensors experience noise, which introduce elements of uncertainty into measurements. Noise can limit the precision of a sensor, making it difficult to distinguish between close values.
- **Resolution:** The design and materials used in traditional sensors limit its ability to resolve fine details. For example, a thermometer with a thick mercury bulb may not be able to detect minute changes in temperature with the same level of accuracy as a more

[72] https://www.citigroup.com/global/insights/global-insights/quantum-sensing-tech-s-new-eyes-and-ears

sensitive sensor. Measurement of time is also classed as a sensing application. As an example, a common quartz wristwatch is accurate to within 15 seconds in a month. In comparison, atomic clocks are a type of quantum sensing technology that offer the highest resolution measurement of time possible down to less than $1x10^{-10}$ of a fraction of a second, or less than a tenth of a billionth of a second, yielding an accuracy of 1 second variation in 300 million years.

Often, there's a trade-off between these limitations. Increasing sensitivity can sometimes lead to decreased precision due to amplified noise. Similarly, enhancing resolution might require a bulky sensor design, which can impact portability.

The Advantages of Quantum Sensing

Quantum sensors overcome the limitations of traditional sensors by leveraging unique properties of the quantum world. The superior sensing capabilities offered by quantum technology in some cases is due to several fundamental principles of quantum mechanics: superposition, entanglement, wave/particle duality and atomic energy level structures. These quantum properties make possible the development of sensors capable of unprecedented sensitivity, accuracy, and resolution, thereby opening doors to previously inaccessible measurements. Some sensors, such as atomic clocks, manipulate energy levels of atoms to achieve their measurements. These differing capabilities enable quantum sensors to achieve accuracy-levels impossible with classical physics.

Superposition: The quantum principle that allows particles, such as atoms, ions, electrons, or photons, to exist in multiple states simultaneously. In classical physics, a system can only be in one state at any given time. For example, a switch is either on or off, not both. However, in the quantum realm, particles can be in a superposition of states, such as being in two places at once or spinning in opposite directions.

Entanglement: The quantum phenomenon where pairs or groups of particles become interconnected so that regardless of distance, the state of one instantly influences the state of the other. As such, the measurements performed on one entangled particle immediately affect measurements of the other.

Atomic energy level structures: Atoms are composed of a nucleus, containing protons and neutrons, surrounded by a halo or cloud or orbiting electrons. The outermost electrons of an atom of are called “valence” electrons, which is where most quantum sensing occurs. Valence electrons can only exist in discrete energy states. By knowing the energy structure of an atom and manipulating and/or measuring the reaction of a valence electron with light and/or magnetic fields, high precision measurements can be taken, such as the sensing of time and the reception of radio frequency-based signals.

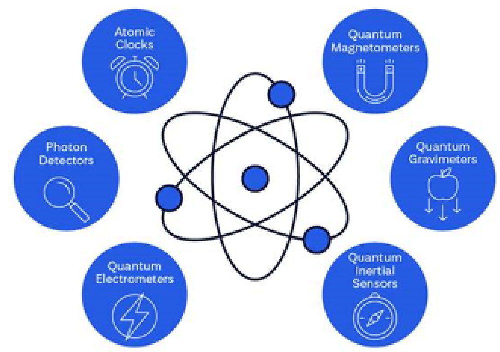
Superposition, entanglement, and the nature of the energy level structures of atoms enable quantum sensors to measure with unparalleled sensitivity and precision, detecting faint forces, such as slight variations in gravitational or magnetic fields. The enhanced sensitivity and accuracy over classical sensors, opens up new possibilities in a number of fields and industries, as discussed below.

Types of Quantum Sensing Technology

Similar to the quantum computing market, quantum sensors are not a monolithic technology. According to Citi Global Insights[73] (see Figure 3) the quantum sensing industry includes a variety of technologies[74]. Complete descriptions of these technologies can be found in the Quantum Economic Development Consortium (QED-C) report on Quantum Sensing Use Cases[75]. Like quantum computing, different technologies are also advancing at different speeds.

Figure 3: Quantum Sensing Technologies

(Source: Citi Global Insights)



Quantum sensing can measure various physical properties and incorporates different materials, each of which provides different benefits to the sensors.

Atomic Clocks measure time with incredible accuracy by using the vibrations of atoms, typically cesium or rubidium, as a "pendulum." Repetitive atomic vibrations enable an ultra-precise timekeeping mechanism. This category of sensors leverages the energy level structure of atoms to function.

- **Applications**: Atomic clocks are crucial to maintain accuracy of GPS satellites, since the smallest error in time measurement can lead to significant errors in determining positions on Earth. In fact, all GPS satellites carry an atomic clock, which provides a timing signal that is accessed anytime GPS is used. GPS also plays a vital role in science, technology, and financial systems that require precise time synchronization. Having an on-site atomic clock, instead of relying exclusively on the timing signal from the GPS satellites, enables GPS resilience in the event of lost, jammed, or spoofed GPS signals, and permits greater efficiencies in data processing for data centers.

Quantum Radiofrequency Receivers use specific high-energy atomic states to sense and receive radiofrequencies with a sensitivity many times greater than current antenna technology with a significantly smaller hardware footprint.

- **Applications**: Quantum radiofrequency receivers allow for the creation of dark communications networks by detecting low strength radio signals below the noise floor of traditional antenna technology. There is also the possibility of replacing current radio tower infrastructure with much smaller, more energy efficient quantum radiofrequency receiver infrastructure.

[73] https://www.citigroup.com/global/insights/global-insights/quantum-sensing-tech-s-new-eyes-and-ears

[74] https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.89.035002

[75] https://quantumconsortium.org/sensing22/

Quantum Magnetometers measure magnetic fields with extreme sensitivity by measuring the strength and direction of materials, like superconducting qubits or atoms in gas, in the presence of magnetic fields.

- **Applications**: Quantum magnetometers are used in applications ranging from detecting submarines, finding buried artifacts, and mining mineral resources[76]. Within medicine, brain imaging techniques, such as magnetoencephalography, also use quantum magnetometer technology.

Quantum Gravimeters measure gravitational forces with high sensitivity. The devices detect minute changes in gravity by observing the behavior of atoms in free fall using techniques related to atomic clocks.

- **Applications**: Quantum gravimeters are used to detect underground structures like tunnels or oil reserves, study volcanic activity changes, and monitor groundwater levels. The devices offer exceptional accuracy in geophysical surveys and underground mapping.

Quantum Gyroscopes measure orientation and rotational motion while **Quantum Accelerometers** measure linear movements. Both are inertial quantum sensors[77]. Quantum gyroscopes and accelerometers use the principles of quantum mechanics to measure motion with high accuracy and precision, often through the behavior of supercooled atoms or photons in a state of superposition.

- **Applications**: Quantum gyroscopes and accelerometers have uses in navigation systems for vehicles, ships, and aircraft, especially in environments where GPS is unavailable, unreliable, or intentionally jammed. The devices are critical for drones, ships, aircraft, satellites, and consumer electronics, and will enable truly autonomous self-driving vehicles.

Quantum Interferometers measure displacement, optical path length, and physical constants by observing the interference patterns of quantum particles like electrons, neutrons, or photons.

The devices leverage the wave-like nature of particles to detect changes in the path length with incredible precision.

- **Applications**: Quantum interferometers are used in scientific research to test fundamental theories of physics and have applications in detecting gravitational waves, measuring the Earth's rotation, and improving the accuracy of optical measurements. Commercial applications can include tunnel detection for defense and border security, underground surveying, oil and gas exploration, and glacier monitoring.

---

[76] https://www.degruyter.com/document/doi/10.1515/teme-2023-0116/html?lang=en

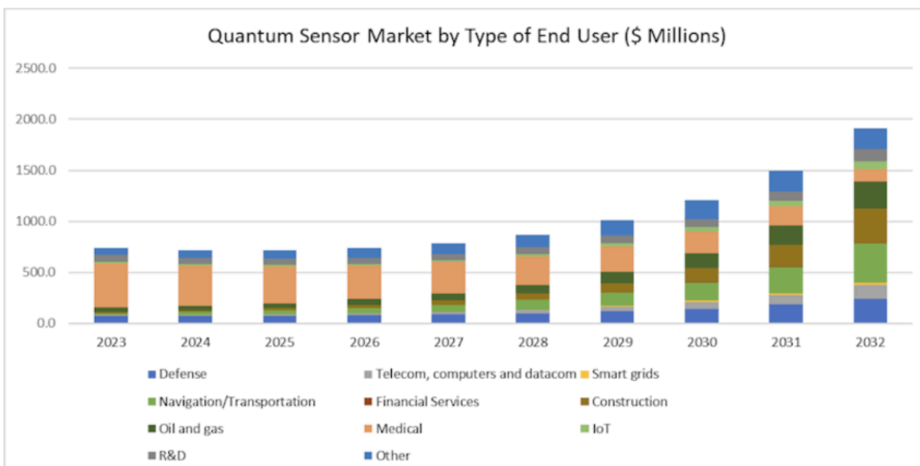
[77] https://www.nktphotonics.com/applications/aerospace-defense/quantum-inertial-sensing/

Quantum sensing technologies offers significant benefits in terms of sensitivity, precision, and the ability to operate in environments where traditional sensors fail[78]. The implications of quantum sensing in commercial industries and national security are profound, making it a focal point of investment and research.

Quantum Sensing Providing Commercial and National Security Value

Quantum sensing capabilities translate to high commercial and national security value across various sectors. As highlighted by Inside Quantum Technologies News (see Figure 5)[79], There are growing number of industries poised to benefit from quantum sensing technology, including navigation, telecommunications, and sustainable energy to name a few.

Figure 5: Industries who can benefit from Quantum Sensing



Commercial Value

The commercial value of quantum sensors resides within its ability to provide unprecedented accuracy and increased sensitivity. Use cases across industries can vary. In this section we will provide a highlight of potential use cases. This is not deemed to be a full list, but instead a small sampling of the types of use cases and applications per industry.

Navigation and Positioning: In addition to improving the accuracy of GPS-free navigation in mining, submarine navigation, and archaeology mentioned above, quantum sensors can lead to

[78] https://royalsocietypublishing.org/doi/10.1098/rsta.2003.1227
[79] https://www.insidequantumtechnology.com/news-archive/iqt-researchs-new-report-estimates-revenues-from-quantum-sensors-to-reach-1-9-billion-in-2032/

safer, more reliable self-driving cars, autonomous drones, and more efficient air travel providing more precise data and enhanced collision avoidance.

Telecommunications and wireless infrastructure: All data centers and network communications rely on a timing signal from GPS for time stamping and synchronization; however, GPS signals are easily interrupted and can cause communications and network outages. Enabled with quantum sensors, telecom networks are more resilient against GPS interruptions by offering a local timing signal for continuous operations. High sensitivity quantum radiofrequency receivers can reduce the physical infrastructure footprint of wireless data infrastructure while increasing energy efficiency.

Medical Diagnostics and Drug Discovery: In healthcare, quantum sensing technologies can lead to the development of highly sensitive imaging tools, enabling doctors to detect conditions at much earlier stages. For instance, quantum-enhanced medical imaging could detect tiny tumors or minute changes in brain activity, revolutionizing early diagnosis and treatment strategies. Rapid analysis of patient DNA, molecular modeling and drug discovery could enable personalized medicines. By detecting subtle variations in a patient's biology, quantum sensors could pave the way for customized and tailored treatment plans.

Environmental Monitoring: Quantum sensors can detect changes in environmental conditions, offering superior data for climate modeling, pollution tracking, and natural disaster prediction. The technology can help monitor volcanic activity, track sea-level rise, or detect pollutants at incredibly low concentrations.

Energy, Resources Management and Sustainability: For oil and gas exploration, quantum gravimeters can detect variations in the Earth's gravitational field, helping to identify oil and gas reservoirs more efficiently, thereby reducing the environmental impact of exploration activities. Just as quantum computers can help with the optimization of renewal energy, quantum sensing can also provide detailed environmental data to drive greater efficiency of renewable energy sources[80]. Atomic clocks situated at data centers can promote lower energy consumption by more efficiently processing data.

Quantum gravimeters can provide crucial data for climate change models by detecting slight changes in water distribution or ice melt by measuring variations in the Earth's gravitational field. Quantum sensors designed to detect single molecules can monitor air and water quality in real-time, thereby identifying pollutants at incredibly low concentrations. These data points can help address environmental health risks more effectively.

[80] https://www.nextgov.com/emerging-tech/2023/04/energy-looks-quantum-sensors-grid-optimization/384755/

National Security Value

According to the Congressional Research Service[81], the Defense Science Board, an independent Department of Defense (DoD) board of scientific advisors, highlights how quantum sensing can provide several enhanced national security capabilities.

Surveillance and Intelligence: Quantum sensors can detect stealth aircraft, submarines, or other vehicles that traditional radar might miss. When mature, quantum-enabled surveillance devices are considered to be able to eavesdrop on electronic communications passively without emitting detectable signals that conventional surveillance techniques rely on. They could also detect electromagnetic emissions which could assist with locating concealed adversary forces, thereby enhancing electronic warfare capabilities.

Secure Communications: Through highly accurate timing and synchronization capabilities, quantum sensors are expected to enhance the security and reliability of communication networks. This is especially critical in scenarios where secure, jam-proof communication is essential, such as military operations or critical national infrastructure control.

Detection of Underground Structures: With their enhanced sensitivity, quantum sensors can detect hidden underground structures, including bunkers and tunnels, from a distance, providing a strategic advantage in military operations and border security.

Enhanced Domain Awareness: The alternative positioning, navigation, and timing options provided by quantum sensing could allow warfighters to continue operating at full performance in environments with low or no GPS accessibility.[82] Quantum magnetometers can detect explosives and other hidden threats with unmatched sensitivity, enhancing security measures at airports, borders, and other critical infrastructure.

Research Value

Beyond commercial and national security, quantum sensing adds value to the advancement of foundational scientific research. Quantum interferometers can test the limits of general relativity and quantum mechanics, potentially leading to new discoveries about the universe. Scientists are also using quantum interferometers to study magnetic and electric fields at the atomic scale to further the development of new materials with tailored properties for electronics, computing, and aeronautics.

[81] https://crsreports.congress.gov/product/pdf/IF/IF11836
[82] https://crsreports.congress.gov/product/pdf/IF/IF11836

Implementation and Challenges

The potential of quantum sensing is vast, but its implementation comes with challenges. Rapid progress of quantum sensing technology is being made to develop portable and robust sensor technology capable of operating in hard environments outside a lab. However, supply chain issues threaten the possibility of high-volume production. If unable to produce at commercial scale, this will limit the ability of quantum sensors to be broadly manufactured and limit their availability for end users.

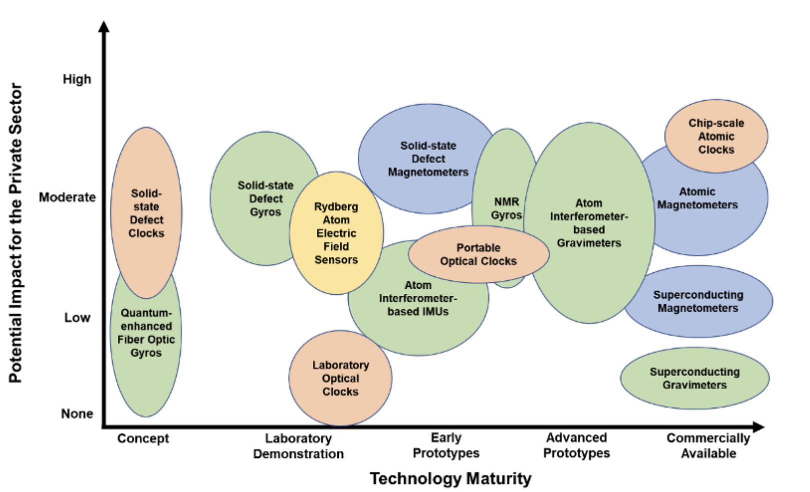
The supply chain of materials, components, and equipment needed to build quantum sensors is widely distributed and possesses multiple points of failure. There may only be a single vendor for a certain element, causing concern over the health of the supply chain. Another challenge is if vendors offer low volume, such that even if a customer had the funding to order thousands of a particular product, the supply chain might not be able to support the order.

Lastly, as with other quantum technologies, there is a need for skilled personnel to operate sensors and interpret sensor data, necessitating substantial investment in education and training. Developing a skilled workforce to build and utilize quantum sensors is needed.

Despite these challenges, the near-term applicability and transformative potential of quantum sensing technology have led to significant public and private investments. Countries and companies are racing to develop and deploy these technologies to capitalize on potential commercial and strategic advantages. As research progresses, and quantum technologies mature, quantum sensing will redefine the landscape of sensing and measurement, with wide-reaching implications across multiple domains.

Technology Readiness of Quantum Sensing

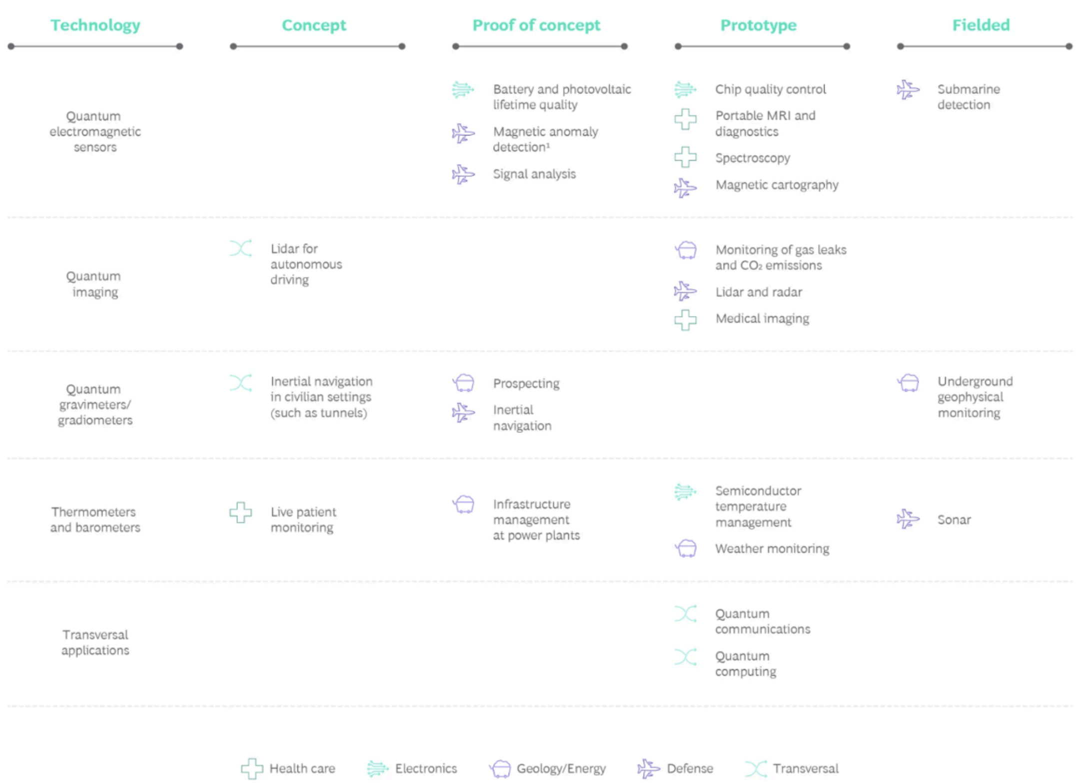
Figure 6: Notional Projected Impact for the Private Sector for Select Quantum Sensors



As with quantum computing, a globally recognized, objective technology readiness level assessment for quantum sensing technology does not currently exist. As such, this section highlights the state of the industry as identified by trusted third parties. QED-C released a quantum sensing report in 2022[83] (*see Figure 6*) which showcased the maturity levels of selected quantum sensors. While still in early development, many quantum sensing technologies have already progressed beyond theoretical concepts. Prototype devices are being tested in both laboratory and controlled commercial environments, such as data centers and aircrafts. The current focus of the quantum sensing industry is to develop practical solutions for specific industries. Companies and research institutions are collaborating to address real-world healthcare, navigation, and security challenges using quantum sensing technology.

According to Boston Consulting Group[84], quantum sensing prototypes for many applications in these industries are emerging (*see Figure 7*), while defense and medical applications appear to be the closest to market maturity.

Figure 7: BCG Assessment of Application Development Levels



[83] https://quantumconsortium.org/sensing22/
[84] https://www.bcg.com/publications/2023/making-sense-of-quantum-sensing

Ongoing research and development efforts by innovative technology companies and research institutions are pushing the boundaries of this transformative technology.

Leading Players:

Tech Giants: Large technology companies like IBM, Google, and Honeywell invest heavily in quantum technologies, including quantum sensing.

Start-ups and Spin-offs: A wave of innovative start-ups and spin-offs from research institutions are emerging, specifically focused on accelerating the commercialization of quantum sensing technologies. Some include Infleqtion, SBQuantum, LI-COR, QuantaLogic, SandboxAQ, and Apogee Instruments.

Academic and Research Institutions: Universities and research labs worldwide play a crucial role in advancing fundamental research and developing quantum sensor concepts and materials. Some research institutions working on quantum sensing include MITRE and the Los Alamos National Laboratory, etc. National Science Foundation (NSF) funded 18 research groups in the U.S. dedicated to quantum sensing.[85]

These efforts highlight the dynamic nature of quantum sensing research.

Select Examples of Ongoing Efforts

Miniaturization and Portability: Companies like QuantaLogic and Infleqtion are developing miniaturized and portable sensors suitable for field applications which can be used for a variety of use cases including medical diagnostics, ordinance detection, telecommunications, etc.

Stability and Scalability: NIST and Harvard are exploring methods to improve the stability and scalability of miniature quantum sensing technologies to integrate with quantum computing and enhanced sensitivity for high-resolution biological sensing.

Room-Temperature Operation: Honeywell and Los Alamos National Laboratory are developing quantum gyroscopes that function at room temperature, eliminating the need for complex cryogenic cooling systems.

Advanced Navigation Systems: Infleqtion, along with researchers from the University of Colorado, demonstrated the world's first software-configured, quantum-enabled high-performance accelerometer by combining machine learning with quantum sensing designed for positioning, navigation, and timing applications.

Enhanced biomedical diagnostics: SandboxAQ is developing quantum and AI technology to increase the sensitivity for diagnosis of cardiovascular disease.

[85] https://thequantuminsider.com/2024/04/13/nsf-invests-29-million-in-18-research-teams-for-quantum-sensing-investigations/

With continued investment and collaboration, we can expect to see significant breakthroughs leading to the development of powerful and versatile quantum sensors that will transform various aspects of our lives.

Quantum Sensing Policy and Recommendations

As the field of quantum sensing matures, governments will need to consider various policy issues. This working group recommends the following policy initiatives:

Funding and research grants: Continued government funding will be crucial for sustained research and development efforts. Additionally, incentives for private sector investment are needed to translate research into practical applications.

Collaboration between government and private sector: Fostering solid partnerships between the public and private sectors is vital for commercialization. Governments and private companies should form joint ventures to co-develop and commercialize quantum sensing technologies to expedite the development and deployment of the technology.

Standardization efforts: Establishing standards will ensure device compatibility and interoperability as quantum sensing technologies mature.

Workforce development: A skilled workforce with expertise in quantum mechanics and related fields is crucial for successfully developing and deploying quantum sensing technologies. Government programs should continue to focus on workforce development for quantum technologies.

Quantum supply chains: Governments should consider allocating funding to support the development of robust quantum supply chains. Doing so will protect national security and enable the growth of a robust quantum ecosystem.

Enhanced international agreements: To ensure a robust and safe supply chain, international quantum agreements should include provisions to protect supply chains.

Continued government support, international collaboration, and effective policy frameworks will be crucial to unlock the full potential of this transformative technology in the years to come.

Chapter 2: Conclusion: A Call to Action for a Future Powered by Quantum Sensing

Quantum sensing stands poised to revolutionize numerous industries with unprecedented measurement capabilities. From revolutionizing healthcare diagnostics to enhancing national security measures, the applications of quantum sensing technology are vast and hold immense potential for economic growth and societal well-being.

However, if we are to reap the full potential of quantum sensors, it is critical to act now while the global race for quantum dominance accelerates. Failing to invest in, develop, and commercialize quantum sensors will result in loss of economic opportunity, harm to national security, and loss of battlefield advantage to adversaries.

> **C-Suite executives:** Explore the potential of quantum sensing for your business. Engage with research institutions and technology companies to understand how this technology can address your industry's challenges and unlock new opportunities. Early adoption positions you as a leader in the emerging quantum economy
>
> **Government policymakers:** Recognize the strategic national security and economic importance of quantum sensing. Increase funding for research and development efforts, help to develop a robust quantum ecosystem and supply chain, incentivize private sector investment, and foster a collaborative ecosystem. By supporting the advancement of quantum technology, you are investing in the nation's future economy, security, and scientific leadership. In the U.S., this means reauthorizing the National Quantum Initiative, which expired in September 2023.

The time to explore the transformative power of quantum sensing is now. We can unlock its potential through collective action and pave the way for a future filled with groundbreaking advancements across all sectors. Let's harness the power of the quantum world and build a better tomorrow.

White Paper

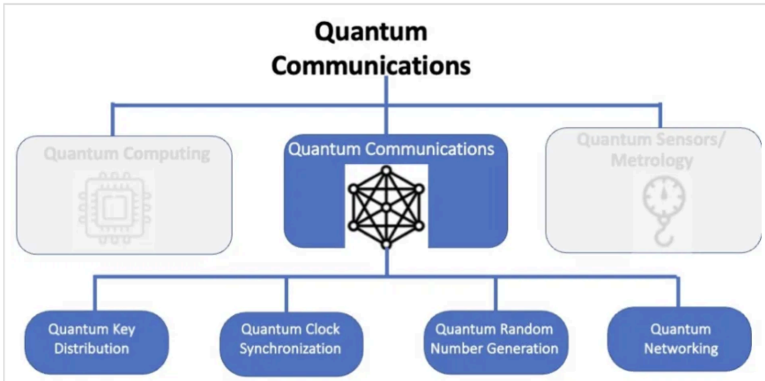
Demystifying the Capabilities of Quantum Technologies Available Today and in the Future

Chapter 3: Quantum Networking & Quantum Communications

ATARC Global Quantum Working Group

Copyright © ATARC 2024

Quantum Networking & Communications



Source: https://steveblank.com/2022/03/22/the-quantum-technology-ecosystem-explained/

With rapid advancements in quantum technologies, it's essential to understand the current and future capabilities of quantum networking and communications. At the forefront is Quantum Key Distribution (QKD), introduced by Charles Bennett and Gilles Brassard in 1984, which uses quantum mechanics to enable unbreakable encryption. QKD marks the shift of quantum theory from abstract science to practical, secure communication methods that differ fundamentally from classical encryption.

Here we explore the state and outlook of quantum networking and communications, demystifying their real-world applications, limitations, and transformative potential.

Quantum technologies exploit quantum physics and quantum mechanical effects which can lead to new capabilities with networking and communications. As highlighted by the U.S. National Quantum Initiative Advisory Committee (NQIAC), "Quantum networking and communication … enable the transmission of quantum states and the distribution of entanglement across multiple quantum information systems. This capability could one day connect quantum devices to build larger-scale quantum computers or distributed quantum sensors with sensitivity that surpasses the standard quantum limit."[86]

Quantum communications utilize quantum states to encode information. The development of these secure communication protocols uses the principles of quantum mechanics (including superposition and entanglement) to ensure the confidentiality and integrity of transmitted information. Quantum networking refers to a type of network that uses quantum bits (qubits) to process and store information. Given the inherent interconnectivities of the two technologies, we will discuss both within this chapter.

86 https://www.quantum.gov/wp-content/uploads/2024/09/NQIAC-Report-Quantum-Networking.pdf

Quantum communications and networking can be pure quantum technologies or hybrid quantum-classical networks. Pure quantum communication and networking technologies are farther away from maturing as the quantum technologies themselves have advancements which need to occur, and therefore most of today's technology are hybrid. These integrate quantum and classical communication channels, leveraging the strengths of both to enhance overall network performance. This approach is practical for gradually transitioning from classical to fully quantum networks.

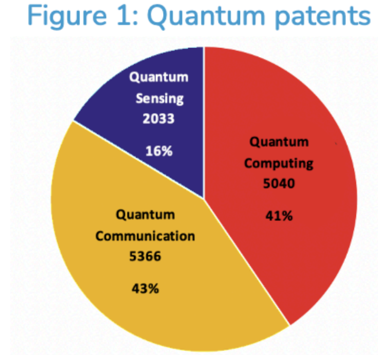
> **Key Concepts in Quantum Networking & Communications**
>
> **Qubits and Superposition:** In classical computing, bits are binary and can be either 0 or 1. Qubits, however, can be in a state of 0, 1, or both simultaneously, thanks to superposition. This property allows quantum computers to process vast amounts of data simultaneously.
>
> **Entanglement:** Quantum entanglement is a phenomenon where two or more qubits become interconnected such that the state of one qubit directly influences the state of another, regardless of distance. This property is crucial for quantum networking, enabling instantaneous communication across long distances.

Mature quantum networking and communications technologies are expected to provide safe and secure communications with a significant impact to national security as these have the potential to 1) improve security through the use of physics-based security that's unhackable; 2) increase computational power through distributed quantum computing networks; and 3) improve precision through distributed quantum sensors.

Global Engagement on Quantum Networking & Communications

Efforts to advance quantum information science, including that of quantum networking and communications, are incorporated into quantum programs around the globe. Quantum communication patents are the largest segment of patents for quantum technologies (see Figure 1)[87]. Included within the quantum communications patents are technologies such as quantum internet, QKD and others. As noted in *Chapter 2, Demystifying the Capabilities of Quantum Technologies Available Today and in the Future Chapter 2: Quantum Sensing*[88], China is leading the efforts for quantum communications patents with over 3600

Figure 1: Quantum patents



[87] https://www.euroquic.org/wp-content/uploads/2024/03/QuIC-White-Paper-IPT-January-2024.pdf
[88] https://atarc.org/wp-content/uploads/2024/07/demystifying-the-capabilities-of-quantum-technologies-available-today-and-in-the-future.docx-3.pdf

patents, and the U.S. is a distant second in patents with approximately 550 patents in quantum communications.

Quantum computing, communications, networking and sensing technologies, while developed individually will not be deployed in silos. Quantum technologies will ultimately interact with each other, and with classical technologies, creating a quantum ecosystem. One illustration of this interconnectivity is with defense implementation. One can see the interconnectivity of quantum computing, sensing, communications and networking as discussed by the Joint Air Power Conference Centre[89]. (see Figure 2)

Figure 2: Quantum Enabled Warfighting

Global leadership in the fields of quantum communications and networking development and deployment is being led by the People's Republic of China (PRC), which has made quantum communications technology a major focus of their quantum programs with a significant patent portfolio dedicated to quantum communication and networking technologies. According to the Information Technology & Innovation Foundation (ITIF) "China has secured global leadership, notably demonstrated through the development of the world's longest quantum key distribution (QKD) network—the 1,200-mile Beijing-Shanghai backbone. Coupled with the groundbreaking Micius satellite, which extends quantum communication over even greater distances, this network has put China at the forefront of secure, long-distance quantum communication."[90] (see Figure 3)

Figure 3: 1,200-mile China Quantum Communications Corridor

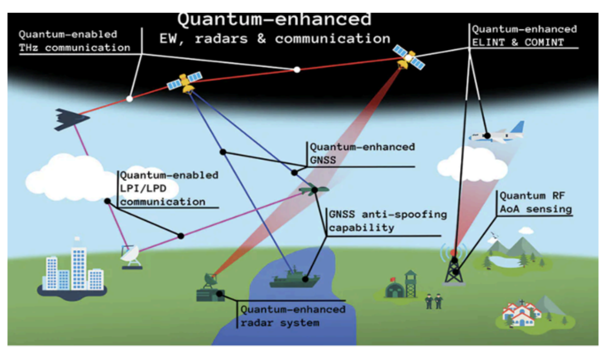
[89] https://www.japcc.org/articles/quantum-technology-for-defence/

[90] https://itif.org/publications/2024/09/09/china-is-challenging-us-leadership-in-quantum-technologies-new-report-finds/

PRC is not alone in its efforts. In Singapore, SPTel and Singtel, communication service providers, are working with Nokia and other companies on strengthening enterprise cybersecurity. In South Korea, a partnership known as the Quantum Alliance, provides an opportunity for companies like SK Telecom and Nokia to work together to develop South Korea's quantum ecosystem. In Japan, an operation centre in Otemachi is connected with three other places that are situated 12, 13 and 45 km away. In Japan a secure TV conference was demonstrated between Kogenei and Otemachi by performing trusted quantum key distribution[91] in 2010.

Early global collaboration was also demonstrated between ID-Quantique, a Swiss company, Senetas, an Australian company, and the University of KwaZulu-Natal in South Africa where they laid the foundation for commercial exploration of QKD. This collaboration began in 2008 and included projects such as QuantumCity and QuantumStadium in Durban, South Africa that showcased early adoption of quantum-secured communication[92]. These initiatives, implemented at demonstrable scale during the 2010 FIFA World Cup and in municipal fiber optic networks, offered valuable insights into the robustness of QKD systems in real-world, commercial environments. This momentum has contributed to the broader scope of international partnerships under the BRICS International Quantum Communications Research initiative, a multilateral collaboration between Brazil, Russia, India, China, and South Africa.[93]

Figure 4: Joint Air Power Conference Centre



The European Quantum Communication Infrastructure (EuroQCI) Initiative, led by the EU and the European Space Agency, is focused on designing, developing and deploying a secure quantum communications infrastructure composed of a terrestrial segment relying on fiber communications networks linking strategic sites at national and cross-border level, and a space segment based on satellites.[94] The EU program aims to safeguard sensitive data and critical infrastructures by integrating quantum-based systems into existing communication infrastructures for QKD, providing an additional security layer based on quantum physics. A European consortium, dubbed Nostradamus, is led by Deutsche Telekom (DT), a digitalization partner for the EU, and includes other partners including the French tech company Thales, and the Austrian Institute

[91] https://opg.optica.org/oe/fulltext.cfm?uri=oe-19-11-10387&id=213840
[92] Realizing long-term quantum cryptography
[93] BRICS International Quantum Communications Research Underway
[94] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

of Technology. The consortium is developing EU's quantum communications testing infrastructure.[95] Through the EuroQCI program, Nokia is working with the national research and education network of Greece, GRNET, the HellasQCI consortium to advance a nationwide quantum-safe network infrastructure.[96] There are other activities as well including a partnership with Nokia and Belgium communications service provider Proximus that completed a live trial of QKD by successfully encrypting and transmitting data between data centers in Brussels and Mechelen. In Portugal, IP Telecom is establishing quantum-safe connectivity for Portugal's three major data centers. In the report by the Joint Air Power Conference Centre, Dr. Michal Krelina has highlighted the importance of precision of quantum clocks within a quantum-enhanced communications infrastructure for defense purposes, and validates the interconnectivity of the different quantum technologies. (see Figure 4)[97]

In the United Kingdom, the government is asking industry for key commercial opportunities, technology requirements and milestones for quantum including quantum networking. The quantum networking call is asking for technology and research milestones to materialize quantum networks, analysis of competing quantum networking components, underpinning classical infrastructure requirements to inform ongoing policy developments, government, and infrastructure developments programs.[98]

In Canada, TELUS Corporation is partnering with quantum computing company Photonic to boost next-generation quantum communications. By providing Photonic with access to its fiber-optic network, TELUS will support the testing of innovative quantum technologies to improve the country's digital infrastructure.[99]

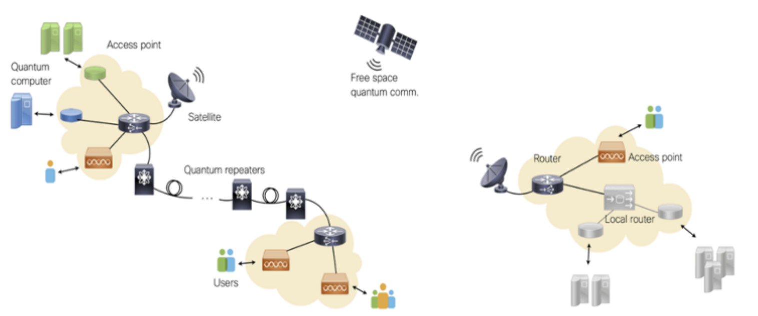
U.S. engagement on quantum networking and communications remains concentrated within the research domain, with a few exceptions. From 2019-2024, the U.S. Department of Energy (DOE) created five different quantum centers, and Q-NEXT is focusing on communications and networking. Q-NEXT research is focused on control and distribution of quantum information enabling secure communication over long distances using quantum repeaters and quantum sensors to achieve unprecedented sensitivities.[100] Q-NEXT has launched two national foundries for quantum materials. Another effort has begun in Tennessee with EPB of Chattanooga, an electric power distribution and telecommunication company, who has partnered with Qubitekk[101] and Oak Ridge National Lab to create the first U.S. commercially available quantum network. This network is designed for private companies and government

[95] https://www.sdxcentral.com/articles/news/eu-invests-200m-in-quantum-technology-to-secure-communications-networks/2024/01/
[96] https://www.forbes.com/sites/nokia-industry-40/2024/08/12/quantum-computing-is-coming-heres-what-needs-to-happen-first/
[97] https://www.japcc.org/articles/quantum-technologies-for-air-and-space/#:~:text=The%20average%20Technology%20Readiness%20Level,and%20are%_20demonstrating%20impressive%20results
[98] https://www.contractsfinder.service.gov.uk/notice/b1a5b405-9df5-4c0e-a4da-293969433080?origin=SearchResults&p=36
[99] https://finance.yahoo.com/news/telus-photonic-collaborate-boost-quantum-145300385.html
[100] https://nqisrc.org/
[101] https://qubitekk.com/epbquantumnetwork/

to run quantum equipment and applications in an established fiber optic environment. This project is aimed at accelerating the process for bringing quantum communications technologies to market.

The DOE announced[102] a private-public partnership dedicated to quantum and space with one of the objectives being to integrate and orchestrate a quantum secure communication demonstration in orbit. Also in the U.S., Cisco Quantum Lab has been established to work with universities and start-ups to develop the quantum frontier of networking and security. (see Figure 5)

Figure 5: Quantum Networking focus from CISCO



NASA announced sending quantum communications to the international space station. As part of the SpaceX 31st commercial resupply mission, NASA sent the Space Entanglement and Annealing Quantum Experiment, or SEAQUE, from the Jet Propulsion Laboratory in southern California to the international space station. SEAQUE is a technology demonstration that will explore how quantum technologies can improve communications across vast distances. If successful, the experiment may pave the way for quantum communication systems globally and in space.[103]

Engineering quantum systems are advancing at a rapid pace, and researchers are looking to unleash the power of quantum technologies for secure communications and networking. Future fault-tolerant quantum computers, which aren't expected for many years, are expected to break the legacy public-key encryption systems, but today's advances in Post-Quantum Cryptography (PQC) algorithms, which are classic and not quantum technologies, can provide an answer to this cybersecurity threats. But many are looking at quantum solutions along with PQC efforts. The need for safe communications has expanded with the rapid growth of the Internet of Things. This amplified demand calls for new sources of randomness for security, and that is where quantum random number generators can provide a solution. In addition to direct applications, the underlying optical and photonics hardware technologies could find dual use for next-generation classical optical products, something Cisco is planning to leverage. Both a near-term market horizon and the value of the corresponding

[102] https://www.energy.gov/technologytransitions/articles/us-department-energy-announces-first-its-kind-collaboration-quantum
[103] https://science.nasa.gov/biological-physical/investigations/seaque-space-entanglement-and-annealing-quantum-experiment/

optics/photonics technologies make networking and security a sweet spot for investment in quantum technologies.

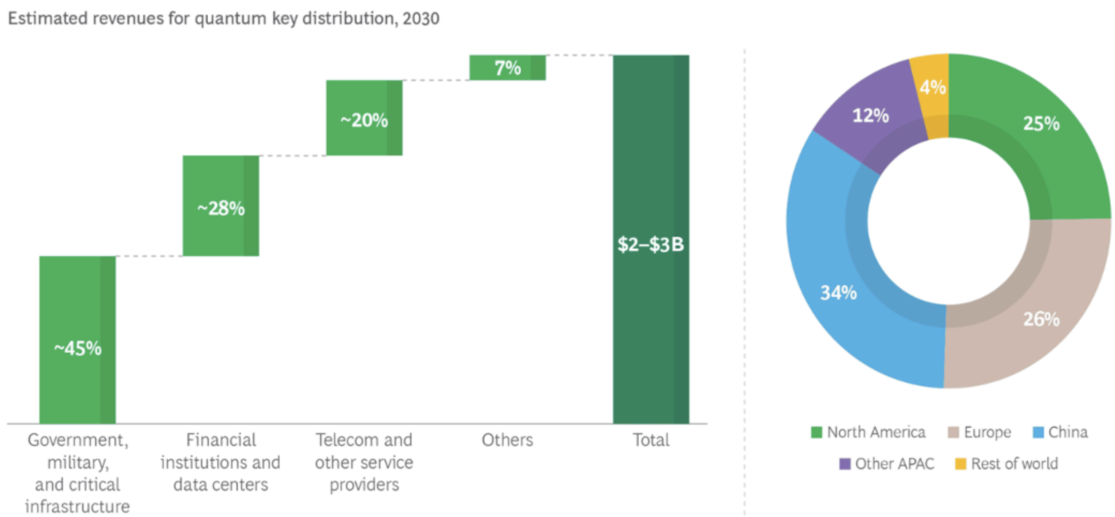
Quantum Networking and Communications Technologies

As with quantum computing and quantum sensing, there is no one monolithic technology that covers networking and communications. Key distribution and random number generators are both used in cryptography and data security, but they have different purposes and methods and are different than the post quantum cryptography (PQC) algorithms which use classical computing and not quantum mechanical effects. Below is a high-level discussion of the different networking and communication technologies, the use cases, and their readiness levels.

Quantum Key Distribution (QKD): Authentication protocols in quantum networks ensure that communicating parties are genuine and not adversaries. Quantum authentication schemes often combine classical cryptographic techniques with quantum mechanics to provide robust security guarantees. This security is a key focus for QKD technologies. QKD is a secure communication method that uses quantum mechanics to encrypt and decrypt messages. Unlike classical encryption, which can theoretically be broken once a large enough fault-tolerant quantum computer is developed, QKD's security is based on the fundamental laws of physics and deemed to be unhackable. Any attempt to eavesdrop on a QKD process will inevitably alter the state of the qubits, alerting the communicating parties. There are a variety of different industries and use cases for QKD. According to the Boston Consulting Group (see Figure 6)[104] these span many difference areas including finance, defense, health care, telecommunications, etc. China and Europe make up more than half of the key geographies engaging with QKD. QKD's inability to be implemented in software or as a service on a network makes it difficult to integrate into existing network equipment. The U.S. National Security Agency's position is that post quantum cryptography algorithms supported by NIST are more affordable at this time.[105] Both the benefits and detractions of QKD are discussed by the Quantum Economic Development Consortium in their report, QKD: Part of a Defense-In-Depth Security Strategy.[106]

[104] hhttps://www.bcg.com/publications/2023/are-you-ready-for-quantum-communications#:~:text=BCG%20helps%20global%20and%20regional,Public%20Sector
[105] https://steveblank.com/2022/03/22/the-quantum-technology-ecosystem-explained/
[106] https://quantumconsortium.org/qkd-part-of-a-defense-in-depth-security-strategy/

Figure 6: Key Sectors and Geographies for QKD



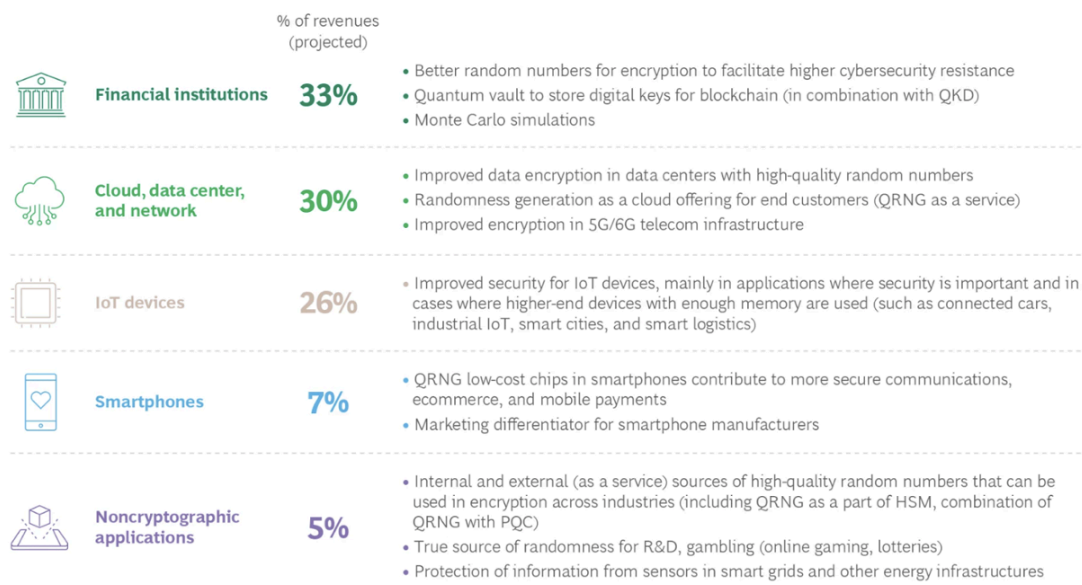
Within QKD, there are different technologies include:

- Device-Independent QKD (DI-QKD): DI-QKD protocols do not rely on the trustworthiness of the devices used in the communication process. This enhances security by eliminating potential vulnerabilities introduced by compromised hardware or software.
- Continuous-Variable QKD (CV-QKD): Unlike discrete-variable QKD, which uses individual photons, CV-QKD employs continuous variables such as the quadrature components of a light field. CV-QKD systems can be more compatible with existing telecommunication infrastructure, leveraging homodyne detection techniques.

Quantum Random Number Generators (QRNGs): Quantum random number generators are a hardware component that generates unpredictable random numbers using quantum mechanical effects. QRNGs are used in a variety of applications, including cryptography, data security, statistical analysis, and gaming. QRNGs are considered a root of trust in cybersecurity because they produce unpredictable outcomes in a controlled way. QRNGs are believed to have built in checks for tampering to provide high attack resistance. According to Boston Consulting Group (see Figure 7)[107] there are several industries who can benefit from and have a need for QRNGs including industries that use the Internet of Things, data centers, and financial institutions.

[107] https://www.bcg.com/publications/2023/are-you-ready-for-quantum-communications#:~:text=BCG%20helps%20global%20and%20regional,Public%20Sector

Figure 7: Industries and Drivers for Quantum Random Number Generators



	% of revenues (projected)	
Financial institutions	33%	• Better random numbers for encryption to facilitate higher cybersecurity resistance • Quantum vault to store digital keys for blockchain (in combination with QKD) • Monte Carlo simulations
Cloud, data center, and network	30%	• Improved data encryption in data centers with high-quality random numbers • Randomness generation as a cloud offering for end customers (QRNG as a service) • Improved encryption in 5G/6G telecom infrastructure
IoT devices	26%	• Improved security for IoT devices, mainly in applications where security is important and in cases where higher-end devices with enough memory are used (such as connected cars, industrial IoT, smart cities, and smart logistics)
Smartphones	7%	• QRNG low-cost chips in smartphones contribute to more secure communications, ecommerce, and mobile payments • Marketing differentiator for smartphone manufacturers
Noncryptographic applications	5%	• Internal and external (as a service) sources of high-quality random numbers that can be used in encryption across industries (including QRNG as a part of HSM, combination of QRNG with PQC) • True source of randomness for R&D, gambling (online gaming, lotteries) • Protection of information from sensors in smart grids and other energy infrastructures

Quantum Repeaters: Quantum repeaters are essential for extending the range of quantum communication. They amplify the quantum signals without disturbing their quantum state, overcoming the limitations imposed by signal loss and decoherence over long distances. It is widely believed that a necessary and highly demanding requirement for quantum repeaters is the existence of matter quantum memories.[108] These technologies are in development currently.

Quantum Memory: Quantum memory devices are an enabling technology that stores quantum information reliably. These will be crucial for synchronizing qubits in a network, allowing for complex quantum communication protocols. Quantum memories are key components of quantum communications as they will enable the storing of quantum information and can be used with quantum repeaters to extend the range of secure communication networks. This is important for quantum repeaters, networks and cryptography, and currently in development.

Quantum Internet: According to the University of Chicago, “The quantum internet is a network of quantum computers that will someday send, compute, and receive information encoded in quantum states. The quantum internet will not replace the modern or “classical” internet; instead, it will provide new functionalities such as quantum cryptography and quantum cloud computing.”[109] Researchers estimate that it will take 10-15 years to create an

[108] https://www.nature.com/articles/ncomms7787
[109] https://news.uchicago.edu/explainer/quantum-internet-explained

entangled network of quantum computers. Unlike traditional computers, it's not believed that individuals will own their own personal quantum computers, instead, quantum computers will be cloud accessible (as they are now), but the future quantum internet would link multiple quantum computers together. While the full use for a quantum internet is still theoretical, The quantum internet represents a paradigm shift in how we think about secure global communication.[110] Beyond quantum computing, the quantum internet is thought to be able to keep technology in perfect sync across long distances using quantum clocks. The vision of a fully realized quantum internet involves connecting quantum computers and sensors across a network, enabling advanced applications such as distributed quantum computing, quantum cloud computing, and more efficient and secure global communication. The quantum internet is nascent as it will need mature quantum technology to be fully developed prior to networking them together.

Industries That Could Benefit from Quantum Networking & Communication Technologies

As with computing and sensing technologies, quantum networking and communications technologies can provide needed security which could benefit a variety of different industries. From enhanced security and secure data transfers to fully realized quantum internet, here are a few use cases and industries which have been identified, but future benefits may become more apparent as technologies mature.

- **Energy:** Networking can secure communication between power grid components, such as generators, substations, and control centers. It can also help protect against insider threats and facilitate secure data sharing.
- **Lotteries and Gaming:** Quantum communications can provide random number generation for lotteries and online gaming to ensure a uniform winning probability.
- **Finance:** Quantum computing can aid in finance, especially with its advanced simulation capabilities and optimization calculations, and secure communications networks can provide resilience and security. It can also help credit card companies with security customer data.
- **National Security & Cybersecurity:** Secure communications with QKD and ultimately the quantum internet will provide enhanced cybersecurity for companies and governments. For example, QKD ensures that communication channels are virtually immune to eavesdropping and hacking attempts. This is particularly beneficial for federal agencies handling sensitive data.
- **Materials discovery:** A quantum network can provide enhanced computational power needed for breakthroughs in materials discovery, currently outside the reach of classical computation alone.

---

[110] https://news.uchicago.edu/explainer/quantum-internet-explained

- **Quantum AI:** A quantum network can provide enhanced computational power to drive breakthroughs in next-gen quantum AI.

In the next few years, several sectors like IT, space, research, healthcare and retail can attain fast communication and high-performance computing with quantum networking. The near-term uses of QKD and QRNGs have created a focus, mainly in Europe and Asia, for developing and deploying commercial use of QKD. There is also a growing penetration of QRNG chips in smartphones, tablets, PCs, and data centers. Future adoption is believed to happen with increased integration of QRNG chips in Internet of Things infrastructure and devices. As quantum computing and quantum sensing mature, then additional integration into communications and networking will occur.

Quantum Networking & Communications Key Players

As with all quantum technologies, there are a growing number of organizations, governments and academia developing and testing quantum networking and communications technologies. This list is not meant to be exhaustive, but instead a selected list of players of different organizational sizes and from different regions.

Mid-Large Players

Toshiba Corporation, a Japanese company has created QKD products as well as a Quantum Key Management System for the storage, transmission and routing of quantum keys between the nodes of a quantum-secured network.

QuantumCTek, a Chinese mid-size company specializing in quantum communication products and services. plays a crucial role in China's quantum communication infrastructure. QuantumCTek was founded by a group of prominent scientists, including China's "father of quantum" Pan Jianwei and leading quantum pioneer Guo Guangcan. The company has focused on developing QKD technologies.

Nokia, a Finnish Company is working on a secure quantum internet through several public-private partnerships in Europe and Asia.

Boeing, has announced plans to launch a quantum networking satellite demo in 2026.[111] Boeing plans to deploy a small satellite in 2026 to test technology needed for a quantum internet capable of connecting more advanced sensors and computers worldwide

[111] https://spacenews.com/boeing-plots-2026-quantum-networking-satellite-demo/

Small Players/Start-Ups

Qubitekk, a U.S. company, is working to build a quantum network with the partnership of EPB and Oak Ridge National Lab in Tennessee. Their view is that a commercial quantum network, the common-use equipment, software, and network management must be achieved through the integration of commercially released products offered and supported by industry vendors. Only recently has this been possible due to the growth of the quantum component industry. Reliable commercial qubit sources, single photon detectors, quantum-compatible fiber optic switches, and a variety of other devices and software are now available for procurement and inclusion in a commercial quantum network.[112]

Quantum Xchange, a U.S. start-up provides the Phio Trusted Xchange (TX), a quantum-safe, out-of-band key delivery system. Their technology can support QKD deployments, they are not a quantum communications provider or reseller. Their quantum-safe key exchange supports quantum keys generated from any source (QRNG or QKD) protected by any method.

ID Quantique, a Swiss based company, provides high-performance quantum-safe security with QKD and commercial QRNGs. They are also building quantum sensing technologies. ID Quantique (IDQ) has successfully demonstrated the use of quantum communications in the banking industry to secure data through the use of their QRNG to generate keys for security applications and cryptologic operations, such as authentication, digital signatures, and secure access control

Quantum Bridge, a Canadian, quantum networking start-up that is delivering symmetric key distribution technology that achieves future-proofed security at scale, without asymmetric encryption. They are working on key distribution and have shown long-distance quantum cryptography over 200km will remain secure even with seriously flawed detectors.[113]

Quintessence Labs, an Australian company, is providing QKD, QRNGs and Quantum Key management systems. to provide strong data protection and help organizations build a quantum-safe future.

---

[112] https://static.epb.com/sha-930d7f7/assets/quantum/documents/2211.14871.pdf
[113] https://arxiv.org/abs/1109.1473

Academia/National Labs

Quantum Collaborative includes Arizona State University supports research harnessing end-to-end entanglement for quantum networking. They work with industry partners including IBM, Dell and Quantinuum.

TNO, the Netherlands organization for applied scientific research has announced collaborating with Airbus Central Research and Technology to contribute to the Quantum Internet for advancing quantum communications and networking.

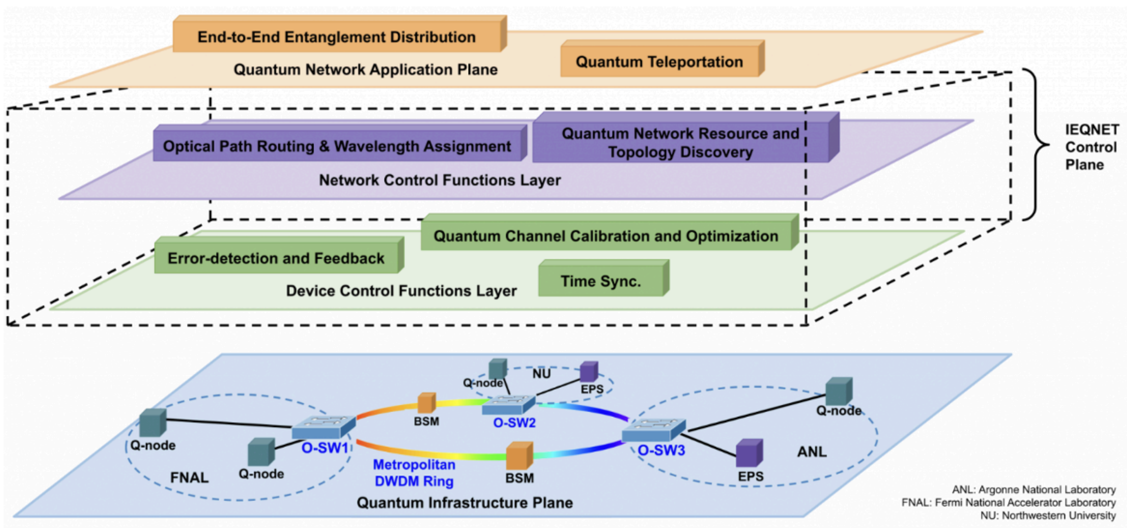
Oak Ridge National Lab, in the U.S., is creating quantum key distribution technologies as well as developing the fundamental building blocks for realizing quantum sensor networks, quantum repeaters and ultimately, a future quantum internet.

Fermi National Lab, in the U.S., is working on a control panel to enable a quantum internet. (see Figure 8)[114] Fermi also received funding from the Department of Energy for developing a nationwide quantum network through the Advanced Quantum Networks for Scientific Discovery (AQNET-SD) project[115]. AQNET-SD researchers are working to develop several technologies and protocols to establish and optimize a quantum network between Fermilab and Argonne National Laboratory using quantum-encoded photons, the particles that transmit quantum information. Also included in this project are University of Illinois at Urbana-Champaign and Northwestern University.

---

114 https://news.fnal.gov/2023/02/nobel-winning-experiment-enables-fermilab-led-quantum-network/
115 https://news.fnal.gov/2023/10/fermilab-receives-doe-funding-to-further-develop-nationwide-quantum-network/

Figure 8: Illinois-Express Quantum Network, or IEQNET, led by Fermilab



IEQNET's quantum networking architecture relies on three planes: an infrastructure plane (connectivity of physical devices), a control plane (control of individual devices and the network as a whole), and an application plane (end-to-end networking services). Image: IEQNET

Challenges Facing Quantum Networking and Communications

Despite its promise, quantum networking and communications technologies face several challenges. Many are similar to challenges facing quantum computing and sensing, but others are unique such as the need for long-range quantum entanglements required for advanced quantum networking and communications infrastructures to be operationally deployed.

Scalability: Developing scalable quantum networks requires overcoming significant technical hurdles, including the integration of quantum components and the development of robust quantum repeaters and memory.

Error Correction: Quantum systems (computing, sensing, communications and networking) are highly susceptible to errors due to decoherence and other quantum noise. Developing effective quantum error correction methods is essential for reliable quantum communication. Intentional introduction of noise is also a potential attack vector given the extreme sensitivity to noise. Ability to prevent noise and distinguish natural noise from artificial noise is important. Characterization of noise is critical for QKD /QRNG applications since the 'noise' is actually a desirable aspect. There are advancements in error correction being made by industry and researchers, but a full-error corrected system is still many years away.

Standardization: As the field is still in its infancy, there is a need for standardization in quantum networking protocols and hardware to ensure interoperability and widespread adoption.

Advancements are needed in the quantum networking architecture technologies as well, those include:

Quantum Teleportation: Quantum teleportation[116] is a process by which the state of a qubit can be transmitted from one location to another, without physically transferring the qubit itself. This is achieved using entanglement and classical communication. It's a fundamental protocol for quantum networking, enabling the transfer of quantum information over long distances. This is still nascent technology in the R&D phase. In 2023, researchers were able to teleport quantum information from a photon to a solid-state qubit over a distance of 1km,[117] but longer distances need more advancements in technology.

Photonics and Optical Fibers: Quantum networks often rely on photonics, utilizing light particles (photons) to transmit qubits through optical fibers. There have been some advances in photonic technology[118] but additional scientific breakthroughs are vital for developing practical and scalable quantum networks.

Entanglement Swapping: Entanglement swapping is a technique used to create entanglement between two qubits that have never directly interacted. This is crucial for extending the range of quantum networks, as it allows for the creation of long-distance entanglement by linking shorter entangled segments. Due to the fundamental laws of quantum physics, a classical optical repeater can't be used to regenerate a qubit as it travels through a network. Using a quantum repeater will provide an alternate way of solving the problem without violating the laws of quantum physics. Boeing along with partner HRL Laboratories have been working on developing such a device and plan to launch it in a sun-synchronous orbit in a satellite called Q4S, approximately 550 kilometers above Earth by 2026.[119]

Quantum Transducers: Quantum transducers convert quantum information between different physical forms, such as between optical and microwave photons. This is

---

116 https://www.nature.com/articles/s42254-023-00588-x

117 _https://timestech.in/science-to-technology-of-quantum-teleportation/#:~:text=Long%2Ddistance%20quantum%20teleportation:%20In,1km%20using%_20multiplexed%20quantum%20memories

118 https://www.nature.com/articles/s41377-023-01173-8

119 https://quantumcomputingreport.com/boeing-announces-plans-to-demonstrate-entanglement-swapping-in-orbit/

essential for interfacing quantum processors (typically operating at microwave frequencies) with optical quantum communication channels. Recent progress has notably enhanced their efficiency and bandwidth. For example, efficiencies nearing 80% have been reported.[120]

Node and Link Configuration with Synchronization: Quantum networks consist of nodes (quantum processors or repeaters) and links (quantum channels). The configuration of these elements impacts the network's efficiency, robustness, and scalability. Topological considerations include mesh, star, and ring configurations. In a fully realized quantum network the end computers would be fault-tolerant quantum computers. QuTech is working on realizing an advanced quantum network in the Netherlands with quantum nodes placed at Delft, The Hague, Leiden and Amsterdam.[121] The goal is for these nodes to function as end nodes as well as quantum repeaters. Synchronization in quantum networks involves aligning the timing of quantum operations across nodes. Precise synchronization is crucial for operations like entanglement swapping and quantum teleportation, ensuring coherent interactions between qubits.

Chapter 3: Conclusion a Call to Action to Advance Quantum Networking and Communications

Quantum networking and communications, along with all quantum technologies, has tremendous implications for the future. It will fundamentally change how we secure data, and security in our technology-driven world means everything. Losing that security – and our privacy – can have devastating consequences.

Understanding these advanced technical aspects and supporting research advancements in the different quantum technologies through government programs and public-private partnerships should be a focus on international collaboration of like-minded governments. Enhanced maturity will be enabled through advanced research, involvements in testbed programs to accelerate technological advancements.

Quantum networking holds the potential to revolutionize secure communications and data transfer, with significant implications for national security, scientific research, and advanced technology development. It can provide needed security for critical infrastructure and our financial institutions as well as provide advancements for national security and commercial industries. While challenges remain, ongoing research and development are steadily paving

[120] https://www.nature.com/articles/s41566-022-00959-3

[121] https://www.tudelft.nl/en/about-tu-delft/strategy/vision-teams/quantum-internet/basics-of-quantum-mechanics/the-six-stages-of-quantum-networks

the way for a future where quantum networks play a critical role in our communication infrastructure.

We recommend that the U.S. government continue to support the advancement of quantum technologies through the National Quantum Initiative Act, and other legislative initiatives. The global supply chain and engagement of quantum technologies also indicates the need for like-minded governments to work together to advance and enhance our security and communications. Lastly, advancing quantum technologies should be through public-private partnerships and should include businesses of all sizes, as many of the innovations within quantum technologies are coming from small, non-traditional government contractors, as well as from larger organizations.

Compilation Conclusion

Quantum technologies comprise a wide range of different types of technologies, each of which is advancing at its own pace and has different capabilities, strengths, and weaknesses. Moreover, today, and in the future, will be hybrid where classical technologies are working synergistically with quantum technologies. While there have been advancements across quantum computing, sensing, networking, and communications, each still has hurdles ahead that must be addressed in order to realize its full potential. Some of these technologies are ready to move out of the lab and into applied applications, while others are still heavily in the research and development phase.

Understanding the technology readiness level and engaging holistically with the quantum and quantum-classical hybrid technology is critical to ensuring U.S. leadership in quantum innovation and global leadership for these critical technologies. The U.S. can begin to harness the power of the quantum world to build a better tomorrow through a few policy recommendations.

Policy Recommendations:

Recommendation 1: Reauthorize and expand the National Quantum Initiative Act:
The National Quantum Initiative Act (NQI) was the first comprehensive quantum policy for the U.S. that expired in September of 2023. Congress must quickly reauthorize this legislation with some needed expansions to ensure domestic quantum policies: 1) are nimble enough to include rapid technology advancements, 2) add a focus on near-term application development while also funding R&D and foundational research, 3) protect the global supply chain with our allies, 4) create testbed and sandbox programs to prove the capabilities for quantum technologies to solve public sector problems, 5) be inclusive of all quantum technologies,

including quantum-classical hybrid, and 6) promote commercialization of domestic quantum technologies.

Recommendation 2: Conduct an objective technology readiness level assessment: Quantum technologies are wide-ranging and there is confusion about the different readiness levels. An objective government review of the technology readiness levels of the different quantum technologies should be conducted and updated on a regular basis to address any confusion relating to capabilities and readiness for deployment and provide transparency of technological advancements.

Recommendation 3: Protect the global supply chain through multilateral agreements: No country owns the entire supply chain for quantum technologies, and therefore we must work with allied nations to protect the global quantum supply chain. The supply chains for each quantum technology can be diverse with single points of failure for critical components. The U.S. government should establish quantum supply chain multilateral agreements to ensure a safe and secure quantum technology supply chain.

Recommendation 4: Invest in quantum upskilling training: Skills gaps have been identified as an area of concern for both industry and government. While the government has established K-12 quantum programs, there should be an added investment in up-skilling the current government and contractor workforce to understand quantum technologies and how they can be deployed for the public sector. These can occur through public-private partnerships to quickly train on quantum coding and use case identification.

Recommendation 5: Programs should be inclusive of all quantum technologies:
Each quantum technology has different strengths and competencies. Quantum programs within the U.S. government should be inclusive of all quantum technologies. For example, quantum computing modalities (annealing and gate-model systems) and qubit architectures (superconducting, ion traps, photonics, etc.) vary and have different readiness levels and capabilities. There is also an expanding arena of quantum-classical hybrid technologies in compute, sensing, communications, and networking. Quantum programs must include the variety of different types of viable technologies (including hybrid). They should also include how these technologies might interact with other emerging technologies such as artificial intelligence, zero trust, and autonomy/robotics. Lack of full engagement can harm the U.S. understanding of these technology strengths, advancements, and limit our ability to benefit fully.

Recommendation 6: Expand programs to develop near-term applications through a quantum sandbox-style program: U.S. programs have mainly been focused on foundational research. This important research should continue, but due to the technology readiness level advancement of some quantum and hybrid hardware and software, government programs must be expanded to ensure they engage with technologies that are now ready to be deployed. A sandbox-style program can provide a safe environment to develop and test applications before they are deployed to address public sector problems. Optimizing public services through quantum technologies could provide needed efficiencies and cost savings.

Recommendation 7: PQC efforts must be agile and ongoing: The government must continue its whole-of-government approach to cryptography and ensure it includes an agile mindset. It is imperative that the government continue its PQC efforts to provide algorithms that can help secure from a cryptographically relevant quantum computing attack. These efforts must continue to engage with industry to ensure US cyber defenses remain resilient and nimble to be able to respond at a rapid pace to a changing threat landscape.

ATARC Global Quantum Working Group

Copyright © ATARC 2025