White Paper

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

ATARC Global Quantum Working Group

March 2024

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. This white paper is intended to be a helpful guidance relating to currently quantum technological capabilities.

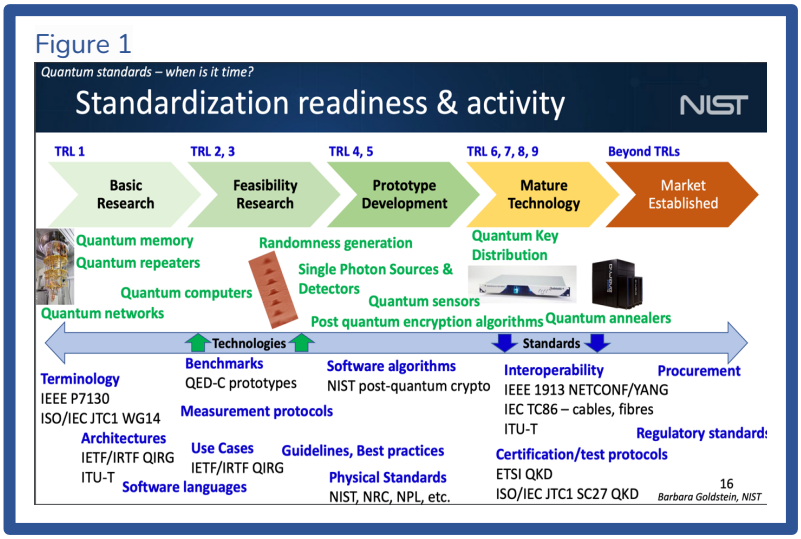
Introduction

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.

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

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]

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.

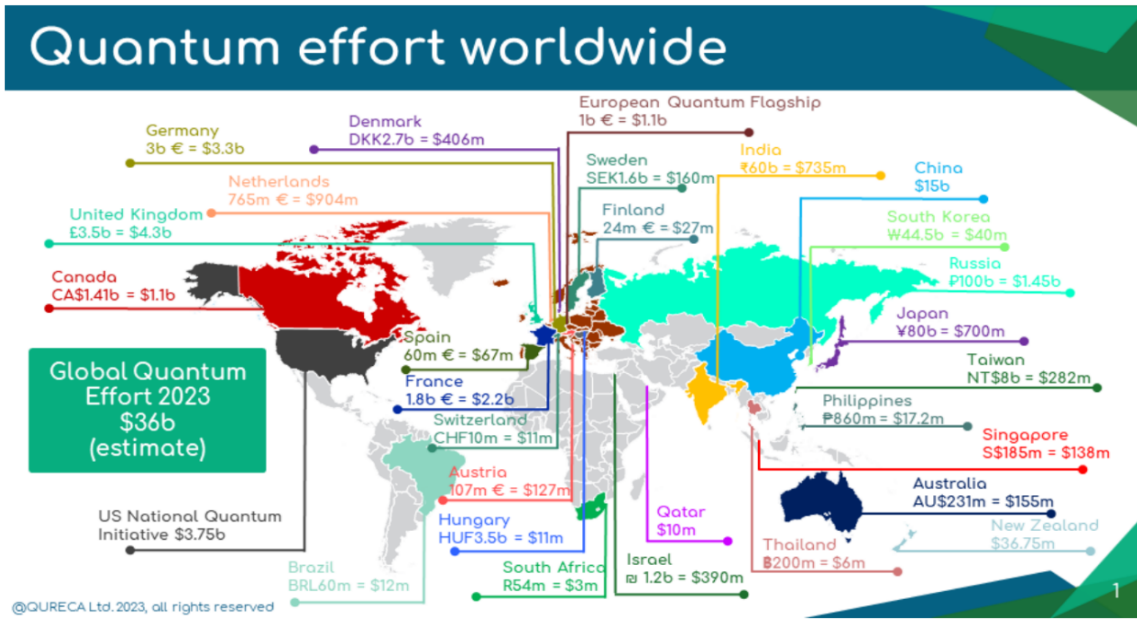
According to Qureca, as of July 2023, worldwide investments in exploring quantum science and technology totals over $36 billion.[6] (*Figure 2*). These government quantum programs support funding for all quantum technologies (computing, sensing, communications, and networking), and support initiatives 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]

[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
[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

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

Figure 2:



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

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.

[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

[12] https://physicsworld.com/a/australia-sets-out-a1bn-national-quantum-strategy/

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.

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.

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)

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.

[13] https://www.quantum.gov/

[14] https://science.osti.gov/Initiatives/QIS/QIS-Centers

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

Chapter 1 – Quantum Computing & Post Quantum Cryptography

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

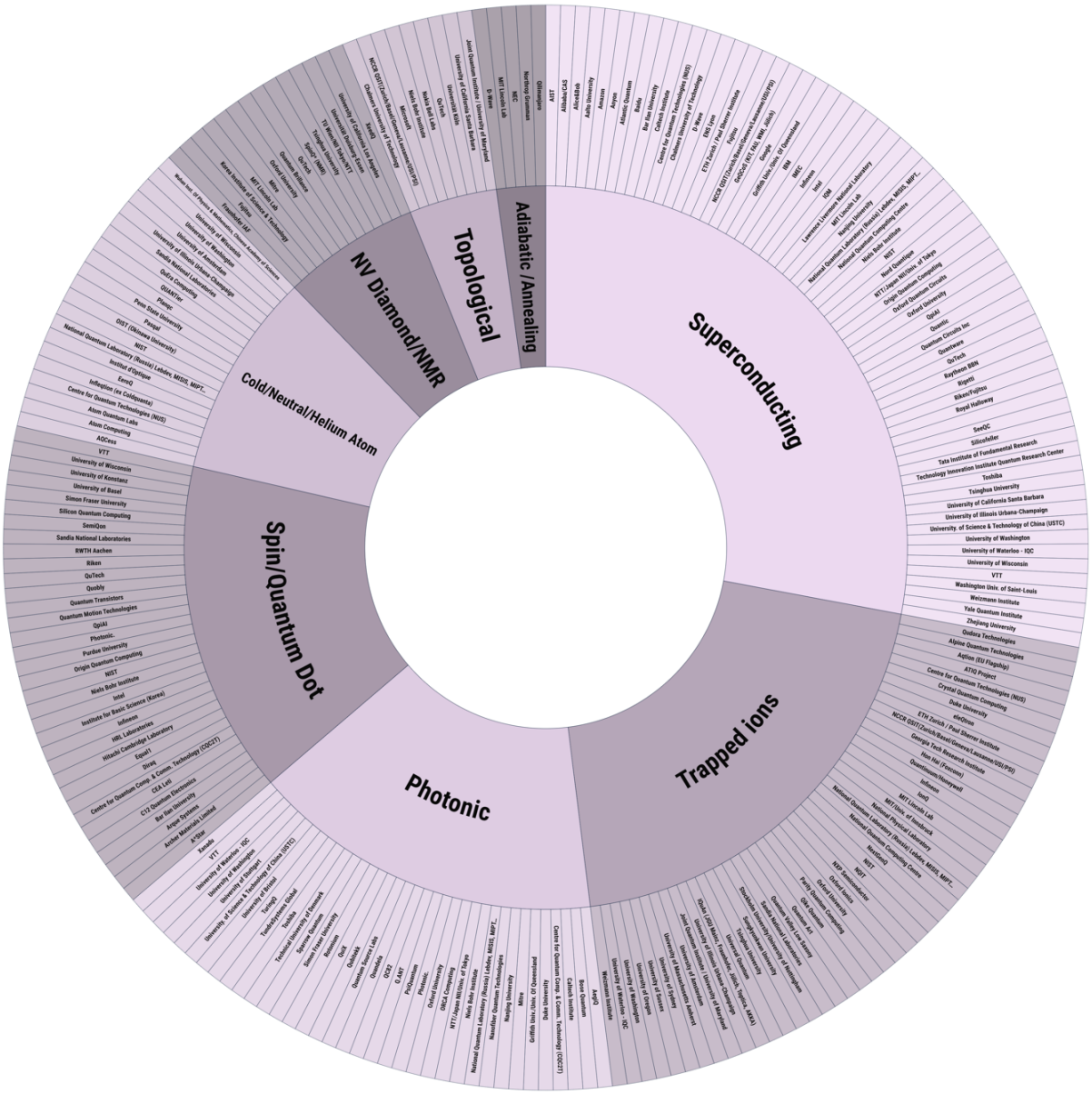
- Under gate-model quantum computing, a quantum logic gate is a basic quantum circuit operating on a small number of qubits which become the building blocks of quantum circuits.
- The method for annealing quantum computing (which is a type of adiabatic quantum computation), is to select optimal solutions 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/

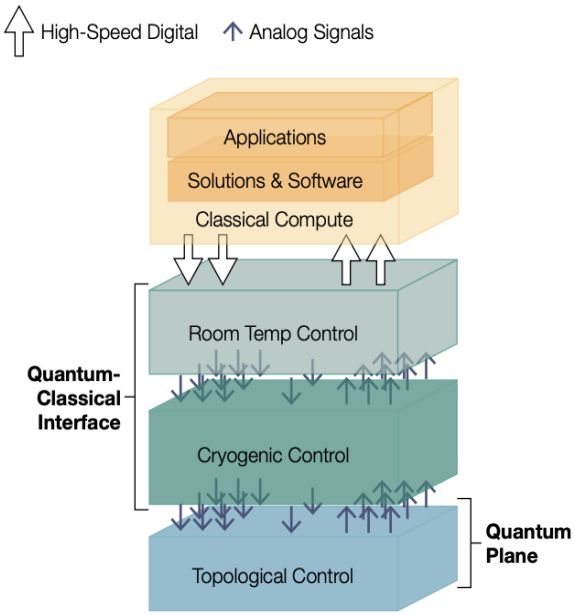
Figure 3

QUBIT MODALITIES / ORGANISATIONS (All types)
by Michel Kurek -2024



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.

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/.

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.

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

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

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 12% and the movement of 60% more cargo. Additionally, the Australian government has announced their intensions 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

[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/
[21] https://rb.gy/cjimpo
[22] https://thequantuminsider.com/2023/06/17/2355920/

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 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

[23] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/early-value-an-introduction-to-quantum-optimizers
[24] https://www.darpa.mil/ARC/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/

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.

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.

[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/

[34] https://uwaterloo.ca/institute-for-quantum-computing/quantum-101/quantum-information-science-and-technology/quantum-simulation

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 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

[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/
[41] https://quantumcomputingreport.com/d-wave-and-zapata-ai-partner-to-develop-solutions-using-quantum-machine-learning/
[42] https://www.nextplatform.com/2021/02/24/glaxosmithkline-marks-quantum-progress-with-d-wave/

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 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.

---

[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.quantinuum.com/usecase/fornetix
[47] https://pmt.honeywell.com/us/en/about-pmt/newsroom/press-release/2023/09/honeywell-leverages-quantum-computing-encryption-keys-to-bolster-utilities-data-security-against-cyber-threats

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 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

[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/qhhnqkuv/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

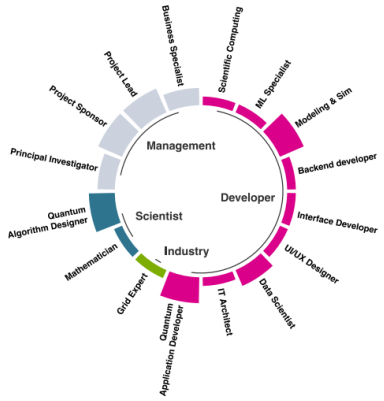
models. However, larger-scale forecasting will need larger, more coherent, systems which are still a few years away.

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 be 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.

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)		

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.

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.

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

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.
- **Talent:** Talent is a challenge for quantum computing companies and end users, including government. The Government Accounting Office released a report[56]

[55] https://techmonitor.ai/hardware/quantum/data-centre-quantum-computer
[56] https://www.gao.gov/products/gao-24-106284

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 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

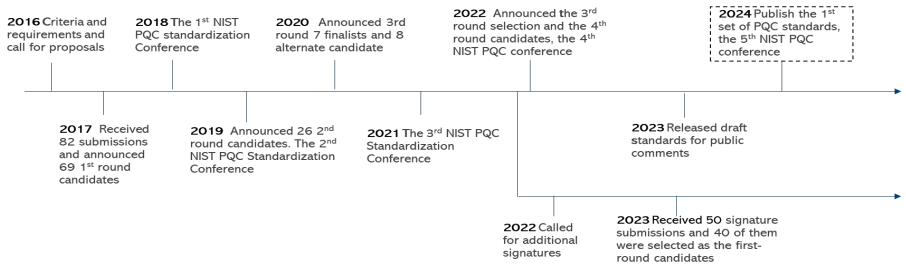
confidentiality, availability, and integrity, potentially leading to unauthorized access, data breaches, and compromised security. The risk is significant enough to warrant proactive measures to adopt and migrate to quantum-resistant encryption methods, ensuring the security of sensitive data in the 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].

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 released the first set of three draft Federal Information Process Standards (FIPS) for public comments which are expected to be published in 2024.

Figure 6



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

[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

Security Memorandum 10 released on May 4, 2022[60] 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.[61] A series of NIST Special Publications 1800-38s is under development and a draft has been released for public comment.[62]

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

- 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.

[60] 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/

[61] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

[62] https://content.govdelivery.com/accounts/USNIST/bulletins/38000a3

- 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,[63]

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

and the Center for Data Innovation[64] 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[65] 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://itif.org/publications/2021/04/27/why-united-states-needs-support-near-term-quantum-computing-applications/

[65] 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/