THE QUANTUM REVOLUTION

A GUIDE FOR ALLIED POLICYMAKERS

Eyck Freymann, Sebastian Orbell, Sophie Coste, and Katharina Klotz

Allied Coordination Working Group • Applied History Working Group

A PUBLICATION OF THE HOOVER INSTITUTION

JULY 2026

The Quantum Revolution

A Guide for Allied Policymakers

Eyck Freymann
Sebastian Orbell
Sophie Coste
Katharina Klotz

Hoover Institution | Stanford University

The Hoover Institution gratefully acknowledges the following individuals and foundations for their generous support of the APPLIED HISTORY WORKING GROUP and this publication:

Blavatnik Family Foundation
Pilar and Lew Davies
Margaret and Daniel Loeb
Amy and Drew McKnight
Roger S. Mertz
Geoffrey S. Rehnert

CONTENTS

Hoover Institution | Stanford University

ALLIED COORDINATION • APPLIED HISTORY

The Quantum Revolution

A Guide for Allied Policymakers

Eyck Freymann, Sebastian Orbell, Sophie Coste, and Katharina Klotz

INTRODUCTION

Quantum technologies are transitioning from laboratory curiosities to strategic systems. Quantum computing, sensing, and communications are beginning to demonstrate utility outside the laboratory. Some are seeing early commercialization and operational testing in defense and intelligence contexts. Capital markets have turned bullish, driving heavy research and development (R&D) investments across the quantum supply chain.

The strategic stakes are substantial. Quantum computers might eventually break the encryption that secures internet commerce, government communications, and military systems, and open new frontiers in materials science and other industrial fields. Quantum sensors promise navigation that cannot be jammed, resource detection that penetrates deep underground, and medical diagnostics at the molecular level. Quantum communications can—in theory—be perfectly secure against eavesdropping.

While quantum technologies have enormous potential, they are challenging for policymakers to grasp. Each technology is progressing on a different timeline, through distinct pathways, and with varying implications for economic competitiveness and national security. Prospects for commercialization remain distant for all of the above applications. The underlying science is technically demanding, sometimes counterintuitive, and often occluded by media hype and industry marketing. Recent progress on fundamental science has been extremely rapid in most areas, but uneven. Benchmarks are fragmented and often vendor specific. No single approach to quantum computing hardware has emerged as dominant.

The research landscape spans dozens of countries, hundreds of companies, and numerous research networks. China is both a competitor and a collaborator. China's quantum strategy is opaque, but Beijing clearly believes the technology has significant geopolitical implications. If classical computing is any guide, the future of quantum technology will be shaped fundamentally by geopolitical rivalry.

WHY THIS REPORT IS DIFFERENT

This report provides a comprehensive assessment of where quantum technologies stand today, how they are likely to develop, and how they

A Hoover Institution Report

July 2026

connect with strategic competition with China. It is written for policymakers in allied countries without a technical background who would like to understand the ecosystem in some depth.

We approach quantum technologies with a *historical perspective*. We explore comparisons and contrasts with classical computing, including in areas where analogies to classical computing may be misleading. We also use extrapolations from recent trends to benchmark how far certain technologies may be from commercial and military use. Whenever possible, we characterize China's quantum strategy using high-quality primary sources in the original language.

We look at three distinct but interconnected topics:

Quantum computing (QC) exploits quantum mechanical properties—superposition, entanglement, interference—to perform calculations that are intractable for classical computers. The most consequential applications involve (1) simulating quantum systems for materials and drug discovery, (2) solving certain optimization problems, and (3) breaking current cryptographic protocols. Today's quantum computers remain small, error-prone, and unable to outperform classical systems on practical tasks. However, several composite metrics have improved extremely rapidly, and early error-corrected scaling is emerging. Under aggressive assumptions, fault-tolerant systems could appear in the 2030s. China's leading expert said in 2025 that he is "hopeful" that China can build one by 2035.[1] But even a marginal slowdown in the pace of progress could push back this date by many years.

Quantum sensing (QS) uses quantum effects to measure time, magnetic fields, gravity, rotation, and other physical quantities with precision beyond classical limits. Applications range from navigation systems that resist spoofing and jamming to geological surveys that reveal subsurface resources to medical devices that detect disease at the cellular level. Unlike quantum computing, quantum sensors are already demonstrating practical advantages in laboratory settings and are beginning to transition to field deployment.

Quantum communications (QComm) aims to transmit information in ways that are fundamentally secure against eavesdropping. Current quantum key distribution systems can detect surveillance attempts, but they are range limited and depend on classical control and authentication planes that remain attackable. The long-term goal is end-to-end quantum networks, but these will require underlying technical advances.

These three quantum technologies are developing on different timelines, but they could potentially interact in significant ways. We cover them first separately and then together.

WHY QUANTUM MATTERS NOW

Three factors make quantum technologies strategically urgent despite their technical immaturity:

1. *The cryptographic timeline is compressing.* Quantum computers capable of threatening today's public-key cryptography might emerge in the 2030s, potentially before post-quantum cryptography is fully deployed.[2] Any encrypted data that is collected today could be *retroactively decrypted* once sufficiently powerful systems come online. If this scenario comes to pass, the geopolitical and ethical stakes will be enormous and the consequences wide-ranging.
2. *Early advantages compound.* In QS, first-mover advantages in data collection and pipelines can create durable moats. Spoofing- and jamming-proof quantum alternatives to GPS are on the rise. In computing,

dominant platforms can shape interfaces and standards for years. In communications, early high-assurance links could be decisive in crisis scenarios.

3. *Today's choices about standard-setting have long tails.* In classical computing, technical standards emerged after decades of diffusion. Quantum technology is developing during a period of intensifying strategic rivalry. Decisions made now on research partnerships, technical standards, and access models will have lasting consequences.

A MULTIPOLAR COMPETITION

Unlike in artificial intelligence, the quantum landscape defies simple great-power narratives. Leadership varies by domain and remains geographically distributed.

The United States leads in QC platforms and cloud-based access. It has the largest venture capital and developer ecosystems, and it leads in publications on QC. It is also competing for the lead in QS.[3]

China has mounted the most extensive QComm deployments, including satellite-based links spanning thousands of kilometers.[4] The practical security benefits of these networks are debatable,[5] but China is clearly determined to preserve its lead in QComm. China also appears to be running a strong second on QC[6] and is in a three-way competition for the lead in QS.

Qubits capture most of the attention in quantum computing, but the supporting infrastructure is equally important—and far more diverse than commonly understood. Enabling technologies help bridge the classical and quantum worlds. They include cooling systems, control electronics, and software stacks, but also a wider array of specialized components: application-specific integrated circuits (ASICs) for real-time error decoding and control, high-speed spatial light modulators, electro-optic and acousto-optic devices, nanophotonic systems, and single-photon detection technologies, including electron-multiplying charge-coupled devices (EMCCDs), single-photon counting modules (SPCMs), and single-photon avalanche diodes (SPADs). Many of these components remain at the frontier of precision engineering. They represent critical bottlenecks and potential choke points, making them of interest to governments as well as investors. The geographic distribution of these capabilities—spanning the United States, the UK, Europe, Japan, and other allied nations—will shape the strategic landscape as the industry matures.

The final section of this report maps these networks of dependencies. The key conclusion is that the United States must build new coordination mechanisms to align its quantum strategy with those of allies.

A NOTE ON SCOPE AND TECHNICAL DETAIL

This report is written for nontechnical policymakers and strategic planners. Three principles guide our approach:

1. *Strategic clarity over technical completeness* We prioritize what policymakers need to know to make informed decisions about quantum policy. The goal is not a comprehensive description of the technology itself.
2. *Acknowledged uncertainty* We flag points in the analysis where simplifications may mask important nuances, and where there is no expert consensus.
3. *Directional accuracy* We focus on trends and relative comparisons that reflect current expert understanding.

For reasons of space, we omit discussion of several notable topics. We do not examine the academic research ecosystem in detail. We do not discuss quantum algorithms and their mathematical foundations. We simplify some technical comparisons between hardware modalities. We do not cover quantum machine learning, hybrid classical-quantum algorithms, or most software infrastructure beyond basic observations. We do not consider environmental impacts, including the energy consumption of cryogenic systems and rare isotope extraction. Finally, we largely bypass the ethical implications of quantum computing for privacy, surveillance, and information warfare.

THE STRUCTURE OF THIS REPORT

Part 1 introduces the fundamental concepts of quantum computing—how it works, why it matters, and the technical hurdles to practical utility—surveying competing hardware approaches and the race toward fault tolerance.

Part 2 analyzes performance trends and commercialization prospects. It assesses whether or not a Moore’s law–like dynamic is emerging in quantum and, if it is, what that implies for timelines.

Part 3 examines quantum sensing and communications, which are probably closer to commercial and military deployment than quantum computing. We focus here on near-term applications, especially navigation, resource detection, and secure communications.

Part 4 explores the geopolitical dimensions of quantum competition. It maps national strategies, collaboration patterns, talent flows, and supply chain dependencies. It also explains why coordinating export controls and achieving supply chain security may be harder for quantum than for semiconductors.

1: FUNDAMENTALS OF QUANTUM COMPUTING

Quantum computing is advancing rapidly. It has the potential to transform a range of high-impact fields—from materials science and biomedical research to cryptography and logistics. But despite technical breakthroughs and growing private investment, the field remains precommercial. The underlying physics is fundamentally different from that of classical computing. No single hardware architecture has yet emerged as dominant.

QC will not replace classical computers. It may outperform them in specific domains, particularly in simulating quantum systems, solving certain optimization problems, and breaking classical encryption protocols. These capabilities are strategically significant for economic competitiveness and national security. However, the path forward is uncertain. Competing hardware modalities, unresolved engineering bottlenecks, and the absence of a standardized platform make it difficult to predict how—and when—quantum computing will scale. Quantum computers also face competition from classical computers, which are advancing quickly with help from artificial intelligence (AI). Beyond quantum simulation and cryptography, researchers have struggled to identify additional applications where quantum computers offer decisive practical advantages, an algorithmic challenge that may prove as consequential as the engineering hurdles.

FUNDAMENTAL CONCEPTS

Quantum computing is rooted in quantum mechanics, the theory that describes how nature works at atomic scales. The rules are counterintuitive: Systems can exist in multiple states simultaneously, they are fundamentally probabilistic, and measurement changes what's being measured. These effects are typically suppressed by interference at larger scales but can emerge when systems are sufficiently isolated from the environment.

At the core of quantum computing are qubits, or quantum bits.[7] Like classical bits, qubits have two possible states—"0" and "1." But they can also exist in a superposition of both states at once.[8] Qubits can also be entangled.[9] This means the state of one qubit can be mathematically linked to another, regardless of the physical distance between them. These properties enable a level of parallelism that is impossible in classical systems.[10]

Together, the properties of superposition and entanglement make quantum computing a fundamentally different computational paradigm. Classical computers simulate physics using binary logic.[11] Quantum computers, in principle, compute using the same rules that govern the physical systems themselves.

This allows quantum computers to attack problems that are computationally infeasible for classical machines. In particular, QC offers potential advantages in simulating complex molecular interactions,[12] solving hard optimization problems,[13] searching unstructured datasets,[14] and factoring large numbers.[15] The last of these applications has major implications for cryptography.[16]

Achieving these theoretical advantages in practice requires overcoming formidable engineering and mathematical challenges.[17] Today's quantum computers are small, are unstable, and require exotic environments such as extreme vacuum or near-absolute-zero temperatures to function.[18] However, as the following sections show, progress is accelerating. Key breakthroughs in hardware, error correction, and system architecture may be within reach—most likely not within the next five years, but plausibly within the next decade.

THE ALGORITHM PROBLEM

Beyond the engineering challenges of building stable qubits and scaling hardware, quantum computing faces a more fundamental uncertainty: We do not yet know what most quantum computers will be useful for. Shor's algorithm for factoring large numbers and quantum simulation of molecular systems represent clear use cases with transformative potential. But the broader landscape of practical applications remains strikingly sparse. Since Shor's 1994 breakthrough, the field has struggled to identify additional algorithms that offer decisive advantages over classical computing on problems of real-world commercial or strategic value. This is not a hardware problem—it is a mathematical and conceptual challenge that occupies some of the best minds in theoretical computer science. Some experts consider it the binding constraint on the field's long-term significance. Policymakers should understand that, even if fault-tolerant quantum computers arrive on schedule, their ultimate impact will depend on algorithmic discoveries that cannot be predicted or guaranteed.

POTENTIALLY TRANSFORMATIVE APPLICATIONS

While today's quantum computers remain rudimentary, theoretical work and early experiments point toward four broad application areas with transformative potential: quantum simulation, factoring, search, and optimization.

QUANTUM SIMULATION: MODELING NATURE WITH NATURE

The most immediate and compelling application of quantum computing is simulating quantum systems.[19] When traditional computers try to simulate how molecules interact, they hit a wall: Each additional particle doubles or triples the computing power needed. Adding just a few more atoms can turn a solvable problem into one requiring centuries or millennia of calculation. For example, simulating the nitrogen fixation reaction used in fertilizer production would take millions of classical CPUs thousands of years (though this number, of course, is falling rapidly).[20] A modest quantum computer, in theory, could perform the same calculation in hours.

This is not merely an industrial efficiency issue; it is a geopolitical one. In the first decade of the twentieth century, the invention of the Haber-Bosch process detached nitrate production from reliance on Chilean mines. This allowed Germany to sustain its munitions production during World War I despite naval blockades. In a similar way, quantum simulation might eventually help nations break dependence on scarce natural resources by enabling the synthesis of superior artificial alternatives.

This is the original motivation for quantum computing. In 1981, physicist Richard Feynman proposed that to understand quantum systems, we must build computers that obey quantum laws.[21] If this vision is realized, it would revolutionize materials science, drug discovery, and energy systems by enabling precise modeling of molecular behavior and reaction dynamics.

CRYPTOGRAPHY: THE COMING CHALLENGE

Quantum computing also poses a long-term threat to public-key cryptography, which underpins internet security, financial transactions, and state communications. In 1994, mathematician Peter Shor proved that quantum computers could break large numbers into their prime factors incredibly quickly, turning a problem that would take traditional computers billions of years into one

TABLE 1 QUANTUM COMPUTING SPEEDUP BY APPLICATIONS AND *N*-COMPLEXITY OF THE PROBLEM

Algorithm	Classical resources	Quantum resources	Quantum speedup	Quantum computer requirements
Quantum simulation	2^N	$\sim N^6$	Exponential	100+ qubits, millions of gates
Factorization	2^N	N^3	Exponential	200+ qubits, millions of gates
Solving linear systems	N^2	$\log(N)$	Exponential	Millions of qubits and gates
Unstructured search	N	$\sqrt{N}$	$\sqrt{N}$	Millions of qubits and gates

Note: Classical and quantum resources refer to the fundamental elements required to perform computations. Leading QCs have at most a few hundred qubits and a few thousand gates. Speedups marked "Exponential" represent the clearest cases for quantum advantage. "$\sqrt{N}$" speedups (quadratic) are more speculative in practice, as they may not overcome the extreme scale and low cost of classical hardware.

solvable in hours.[22] This would render today's Rivest-Shamir-Adleman (RSA)-based encryption vulnerable.[23]

Although no quantum computer yet has the capacity to run Shor's algorithm at scale, progress in error correction and qubit fidelity is closing the gap.[24] In response, the US National Institute of Standards and Technology (NIST) released new post-quantum cryptography standards in 2024.[25] These are designed to resist attacks by quantum systems but are not yet universally adopted. Importantly, any encrypted quantum-vulnerable data stolen today could retrospectively be decrypted in the future once powerful quantum machines come online.[26]

SEARCH AND OPTIMIZATION: LIMITED BUT PROMISING

Other quantum algorithms can search through unsorted data much faster than traditional computers.[27] This could speed up database searches,[28] machine learning,[29] and other tasks that currently require checking many possibilities one by one (see table 1).

In the field of optimization, quantum algorithms may eventually outperform classical solvers on complex tasks such as financial portfolio management,[30] supply chain scheduling,[31] and energy grid design.[32] However, current quantum hardware has not yet demonstrated a decisive advantage in real-world optimization scenarios. Meanwhile, classical computers, enabled by AI, are getting better all the time.

FIRST-MOVER ADVANTAGE AND STRATEGIC LOCK-IN

While the above applications are speculative, it is possible to imagine how early winners could gain compounding advantages. In materials or pharmaceuticals, a firm that patents a novel compound designed via quantum simulation could potentially gain a competitive moat. In defense and intelligence, states that field quantum decryption or secure quantum communication systems ahead of rivals could alter the balance of power.

Thus, governments and private firms are investing heavily, despite technical and fundamental uncertainty. Although timelines remain long, the race to develop quantum technology can therefore be understood as a form of long-term strategic competition.

HOW QUANTUM COMPUTING WORKS

Quantum computing differs from classical computing not just in speed or scale but also in the underlying architecture of computation. Below is a simplified discussion of how quantum computers are built and operated.

QUBITS: THE BUILDING BLOCK

As we have seen, unlike classical bits, qubits can also exist in a superposition of both “0” and “1” states simultaneously. The properties of superposition and entanglement allow quantum computers to encode more information and explore multiple possible outcomes at once.

Qubits can be made from various physical systems, including trapped ions,[33] superconducting circuits,[34] semiconductor spins,[35] neutral atoms,[36] and photons.[37] These systems are all governed by quantum physics, but they differ in reliability, cost, and scalability (see appendix).

QUANTUM GATES AND CIRCUITS

To perform a computation, a quantum computer must manipulate its qubits. This is done through quantum gates—precise controls that change qubit states, similar to how traditional computers use logic gates to process bits.[38] A sequence of gates forms a quantum circuit, which is analogous to a logic circuit in classical computing.

THE CHALLENGE OF DECOHERENCE AND ERROR

Qubits suffer from various forms of quantum error, including bit flips, phase errors, and cross talk. Even the best quantum processors today have error rates vastly above what would be acceptable in classical computing. One of the key barriers is decoherence—the process by which a qubit loses its quantum state due to interference from its environment. Decoherence is a major barrier to the commercialization of quantum computing. Qubits must be isolated from noise yet precisely controlled. This delicate balancing act often requires cryogenic temperatures and vacuum chambers.

The technologies that deal with these issues, known as quantum error correction (QEC), are therefore essential to all quantum computing. QEC involves a combination of hardware and software tools. The difficulty is that—as readers familiar with Schrödinger’s cat[39] may recall—qubits cannot be copied or directly inspected without destroying their state.[40] To solve this problem, quantum computers spread information across many (hundreds to thousands) imperfect qubits to create one reliable “logical” qubit, like using multiple backup drives to protect important data. The quantum properties linking these qubits allow the system to spot and fix errors without disrupting the calculation.

THE ROAD TO FAULT TOLERANCE

The long-term goal of quantum computing is to build fault-tolerant systems: machines that can run arbitrarily long quantum algorithms while automatically correcting for physical errors in real time.

Fault-tolerant machines will require extremely low error rates and efficient error-correcting codes. Most importantly, they will require millions of stable physical qubits to encode and operate on a relatively small number of logical qubits.

Prototypes such as Google's 2024 Willow chip have begun to demonstrate early error-correction thresholds.[41] However, fault-tolerant quantum computing is probably a multidecade engineering challenge. Until fault tolerance is achieved, quantum computing is unlikely to be commercially viable for many if not most tasks.

Yet hardware scaling alone is not sufficient. Many experts are now confident that Shor-scale machines—systems capable of running Shor's algorithm at meaningful scale—will exist within a decade. The deeper uncertainty is whether or not such machines will be broadly useful. That depends on algorithm development, an area where progress has been surprisingly limited since Shor's 1994 breakthrough. This distinction—between building the hardware and discovering what to use it for—is critical for policy planning.

COMPETING HARDWARE MODALITIES

Unlike classical computing, which coalesced around silicon transistors in the 1950s, quantum computing is still in the exploratory phase. There are several physical systems that can form qubits. No consensus has emerged on which modality will prove dominant. This uncertainty complicates investment and policy planning, but it also drives innovation.

Each type of qubit has different strengths and weaknesses: how long the qubits last, how accurately they operate, how many you can build, how often they fail, and how hard they are to manufacture. While many are still in the lab, several have gained traction with major firms and research institutions.

No modality currently scales efficiently. However, several are advancing quickly (see appendix). Superconducting and neutral atom qubits are furthest along. Trapped ions, spins in silicon, and superconducting cat qubits are emerging as serious challengers. At this early stage, it seems plausible that any of them could become foundational to future quantum systems.

The hardware layer will probably generate the most defensible intellectual property, so the outcome of today's modality race will largely determine which of today's QC companies remain competitive tomorrow. The most adaptable firms are probably the full-stack players, which combine hardware, software, and control infrastructure in-house.

ENABLING TECHNOLOGIES AND THE QUANTUM STACK

Qubits capture most of the attention in quantum computing, but the supporting infrastructure is equally important. Enabling technologies such as cooling systems, control electronics, and software stacks help to bridge the classical and quantum worlds. They represent critical bottlenecks and are therefore of interest to governments as well as investors.

CRYOGENIC SYSTEMS

Most qubit modalities need to operate at temperatures close to absolute zero.[42] They therefore depend on dilution refrigerators. These custom-built systems often cost between $500,000 and $2.5 million, with annual maintenance in the tens of thousands.[43] They rely on helium-3, a rare isotope that today is sourced mainly from nuclear research programs. Helium-3 happens to be abundant on the moon. Commercial fusion reactors might also provide an alternative source, if they are developed.

CONTROL HARDWARE

Quantum control systems are the interface between classical electronics and quantum logic. They initialize, manipulate, and read out qubits using microwave pulses, lasers, or electromagnetic fields. The specific tools vary by qubit modality but include custom ASICs, field programmable gate arrays (FPGAs), microwave generators, precision lasers, spatial light modulators, electro-optic and acousto-optic devices, and single-photon detection technologies (EMCCDs, SPCMs, SPADs). One can think of them as the "nervous system" of a quantum computer, but one that must operate with nanosecond precision while continuously adapting to quantum behavior.

Today's control systems are bulky, power hungry, and often assembled from off-the-shelf components. As systems scale from dozens to thousands of qubits, wiring complexity and latency become constraints. The critical challenges are speed and integration. Quantum error correction requires real-time feedback to detect errors, compute corrections, and apply them within microseconds—faster than qubits lose their quantum state.

Hybrid control systems—which harmonize quantum and classical operations by collocating processing near quantum hardware—are emerging as essential infrastructure. These systems may become the standard entry point for interfacing high-level quantum algorithms and error-correction codes with low-level quantum hardware. These systems depend on sophisticated software integration and rapid round-trip communication with high-performance classical processors (including graphics processing units [GPUs], FPGAs, or ASICs). It is not easy to make the classical and quantum layers of the system communicate seamlessly, though various companies are working on possible solutions.[44]

ERROR CORRECTION AND DECODING

Quantum error correction (QEC) codes are sequences of operations and measurements designed to detect and correct errors in quantum computers. There are several families of error-correction codes. The most prominent are surface codes[45] and quantum low-density parity-check (qLDPC) codes.[46]

Decoding is the crucial process that bridges error detection and correction by analyzing errors and scheduling operations to fix them. Decoders must work faster than errors accumulate across the quantum chip. This requires specialized classical computing hardware and software capable of extremely fast and high-throughput processing, tightly integrated with the quantum control systems.[47] Decoding is a serious bottleneck, particularly as quantum computers scale to thousands or millions of qubits. Real-time error correction will likely involve vast amounts of classical computing.[48]

SOFTWARE AND PROGRAMMING LANGUAGES

At the highest layer of the stack is software. This is where control hardware, quantum logic, and classical processing are integrated into working algorithms.[49] Quantum computers are hard to program. Classical programming models do not translate easily into quantum logic.

The current ecosystem is fragmented. Major players maintain proprietary languages, which are tightly bound to specific hardware architectures.[50] These proprietary languages are very useful for users, but they can create barriers to interoperability. From a strategic perspective, software matters less because it is technically hard to design, and more because of the potential for network effects and lock-in. The history of classical computing shows that foundational software layers (UNIX, x86, CUDA, ARM) often generate durable competitive advantages through developer ecosystems and switching costs.

Quantum algorithms must be translated into error-corrected operations that work with specific quantum hardware. This translation—called compilation and transpilation—acts as the bridge between abstract quantum programs and physical quantum devices.

Today, this process happens mostly within proprietary frameworks developed by individual quantum companies. Each platform has its own language and toolchain, creating silos that limit interoperability. Initiatives such as Microsoft's QIR (Quantum Intermediate Representation) aim to create a common interface. This would allow engineers to implement compilation steps across different platforms and better integrate quantum and classical software components.

The deeper technical challenge lies in discovering new quantum algorithms that are superior to conventional algorithms for useful tasks. The cutting-edge research on quantum algorithms is mostly done by mathematicians and academic computer scientists at universities. Unlike control software, algorithmic breakthroughs cannot be engineered on demand—but the greater the concentration of technical talent, the greater the possibility of sudden breakthroughs. This is another source of uncertainty for policy planners.

STRATEGIC IMPLICATIONS

Quantum computing holds extraordinary long-term potential. It may transform industries ranging from pharmaceuticals and finance to materials science, cryptography, and logistics. But this promise is still distant. Despite breakthroughs in hardware and theory, quantum computers remain precommercial, and the path to scalable, fault-tolerant machines is steep, uncertain, and nonlinear.

The physics is sound. Quantum mechanics enables capabilities that classical computers cannot replicate. The challenge is engineering those principles into reliable systems.

The use cases are compelling but narrow. Simulating quantum systems is the most viable near-term application, especially in fields such as chemistry and materials science. Cryptography (code-breaking via Shor's algorithm) is the other clear use case with proven algorithmic foundations. Optimization and search algorithms are significantly more speculative. The ceiling for quantum computing applications may be extremely high. However, this algorithm problem may prove as consequential as the hardware challenge. Even if fault-tolerant machines arrive by the early 2030s, their strategic and commercial significance will depend on how far researchers can discover applications beyond the current limited set.

Hardware is a key bottleneck. No qubit modality yet satisfies all the criteria for scalable, fault-tolerant computing. The race among superconducting, cat, neutral atom, trapped ion, and spin qubits remains wide open. Scaling physical qubit count while maintaining reliable control and readout remains challenging across all modalities. Wiring and cooling limitations particularly constrain cryogenic approaches.

The stack is still fragmented. Cryogenics, control hardware, and quantum software are evolving in parallel—but without standardization or clear winners, progress remains uneven. This fragmentation creates opportunities for allied nations to establish choke points before the industry consolidates. Just as the Netherlands came to dominate advanced lithography through ASML, middle powers with specialized capabilities in dilution refrigerators, single-photon detectors, or control ASICs could lock in durable positions in the future quantum supply chain. Allied coordination now—before a dominant architecture emerges—could shape the supply chain geography for decades.

There is no obvious "picks and shovels" play. Governments and venture investors that want to bet on quantum face difficult choices about where to allocate capital. It's unclear which hardware modality or software platform will win. As long as this uncertainty remains, quantum companies' valuations will likely fluctuate wildly based on sentiment. Governments that are willing to back an array of deep tech plays will have a structural advantage, and they may seize control of choke points in the QC stack.

The big picture is that QC is not a single race but a set of interrelated races. QC will not achieve its promise until an ecosystem of codesigned hardware, algorithms, and software emerges, with seamless integration between quantum and classical components. It is easy to imagine how the emerging quantum computing ecosystem could come to resemble the mature semiconductor ecosystem, with individual companies building broad moats at each layer of the stack.

In the next section, we examine recent trends in quantum performance benchmarks and extrapolate some more specific lessons about commercialization timelines.

2: COMPUTING TRENDS

While quantum computing remains experimental and precommercial, the fundamental science is advancing at an astonishing pace. If recent trends are sustained, fault-tolerant machines could emerge by the early to mid-2030s, much faster than most forecasts assume.[51] Skeptics will argue that it is unrealistic to expect continued exponential gains, given the complexity of the ecosystem described in part 1.

Today, the best-performing machines still suffer from error rates too high for real-world use. However, hardware improvements are accelerating. The number of imperfect qubits needed to create one reliable qubit is dropping rapidly. Meanwhile, qubits are maintaining their quantum properties for longer periods before breaking down. Quantum volume (QV), the dominant composite performance metric, has improved by a factor of ten annually since 2018.

Nevertheless, even if these trends hold, there is no guarantee that quantum computers will achieve necessary performance thresholds within just a few hardware cycles. QV growth can obscure stagnation in individual metrics. Over the long term, progress across all metrics is indispensable. The challenge for forecasters, governments, and investors is that no qubit modality has emerged as dominant, and benchmarks are fragmented and often vendor specific. This makes it hard to conduct strategic planning and assess who leads and by how much.

Most industry road maps place fault-tolerant systems after 2030. In the meantime, classical systems will probably dominate. Only a few well-capitalized quantum computing as a service (QCaaS) stack players such as IBM, Google, Microsoft, and Amazon currently have the hardware, software, cloud infrastructure, and AI-related services to provide QCaaS.[52] However, due to the wide range of modalities being explored, it is quite possible that a smaller company will land first on a different, more scalable approach.

Market valuations can mislead nonspecialists about the enormous uncertainty around QC's path to commercialization. The sector boomed in 2025, alongside a broader surge in valuations for AI and crypto assets. Skeptics argue that startups such as IonQ and D-Wave that have no clear pathway to profitability should not command valuations in the billions of dollars. Optimists, however, argue that the market is still undervaluing the quantum sector as a whole precisely because of the technical and commercial uncertainty. Policymakers should assume that market valuations will remain volatile.

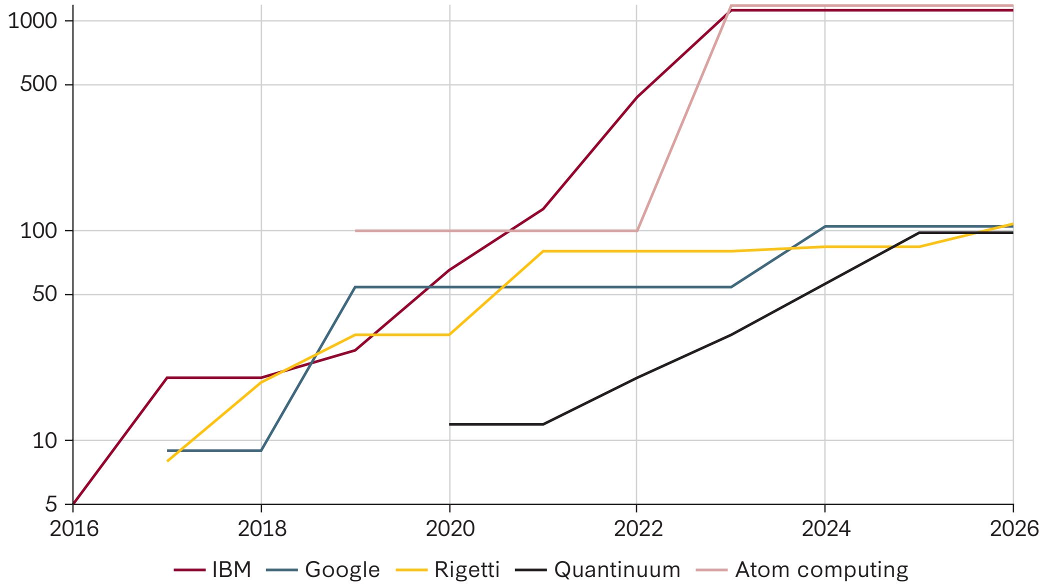
As with classical computing in the 1950s, the race is over intellectual property and strategic leverage over the entire stack. Policymakers and investors should treat quantum computing not as a speculative long shot but as an emerging technology with disruptive potential in specific domains and the possibility of far-reaching impact across the broader economy by the 2030s.

THE ROAD TO FAULT TOLERANCE

Today's quantum computers generally have between fifty and a few hundred qubits and are too error-prone for commercial use, though good enough for research and experiments.[53]

Still, today's systems are opening the door to experimental applications for the first time. Physicists, chemists, and materials scientists are now using quantum computers to simulate small-scale quantum interactions that are difficult for classical machines to model. They are developing new quantum algorithms[54] and optimizing protein folding.[55]

FIGURE 1 Physical qubit count among major hardware players (log scale)



The dominant industry view is that it is on a long road toward fault-tolerant, gate-based digital quantum computers.[56] These future systems will theoretically perform arbitrarily long computations without errors. (Some alternative paradigms have shown commercial promise in narrow contexts. These include analog quantum computing[57] and quantum annealing.[58] But scaling has been a challenge.[59])

Achieving reliable quantum computing requires extremely low error rates—less than one error per hundred operations—and using hundreds or thousands of imperfect qubits to create each trustworthy qubit. For basic chemistry simulations and simple code-breaking, quantum computers need to reduce errors to less than one in a billion operations—a precision comparable to making only one typo in a thousand novels.[60] However, for longer-term applications, including factoring 2048-bit RSA keys and pharmaceutically relevant quantum chemistry simulations, the logical error rate would have to fall by roughly another million times.[61] A commonly cited benchmark is that twenty million noisy physical qubits would be needed to break RSA encryption in under eight hours using Shor's algorithm.[62]

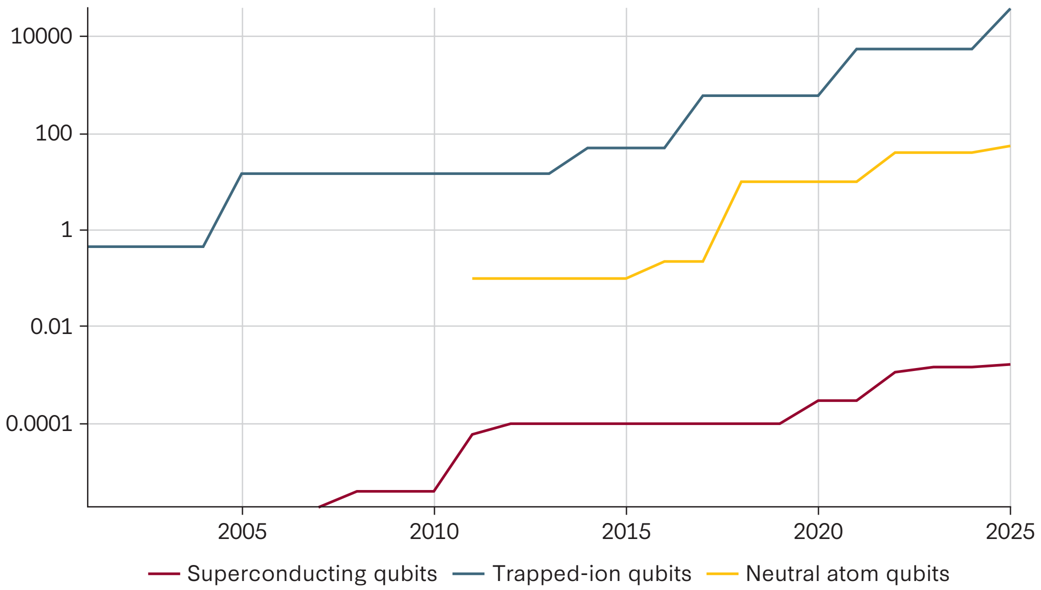
Recent breakthroughs should be understood as stepping stones toward this goal. For example, IBM's 2023 Condor chip reached 1,121 physical qubits. This was the first superconducting device to cross the thousand-qubit mark.[63] Yet Condor was soon retired because error rates were so high that it was unusable for real workloads.

The bottom line is that before quantum computing can be viable for commercial or military tasks, exponential progress is needed across multiple dimensions, including qubit count (see figure 1), coherence time (see figure 2), fidelity, connectivity, and error-correction efficiency. No single benchmark tells the whole story. But taken together, the trend lines are moving in the right direction.

TRACKING PERFORMANCE TRENDS

In classical computing systems, there are standardized performance metrics such as floating point operations per second (FLOPS) and transistor count. By contrast, quantum performance is

FIGURE 2 Qubit coherence time by modality in seconds (log scale)



multidimensional. It varies by hardware modality, application, and error model.

Tracking progress requires synthesizing several indicators and understanding their limitations. Hardware vendors have incentives to publicize benchmarks that highlight their comparative advantage rather than provide apples-to-apples comparisons (see figures 1 and 2). This makes it difficult for investors, governments, or end users to evaluate technological maturity across platforms.

BENCHMARKING QUANTUM PERFORMANCE

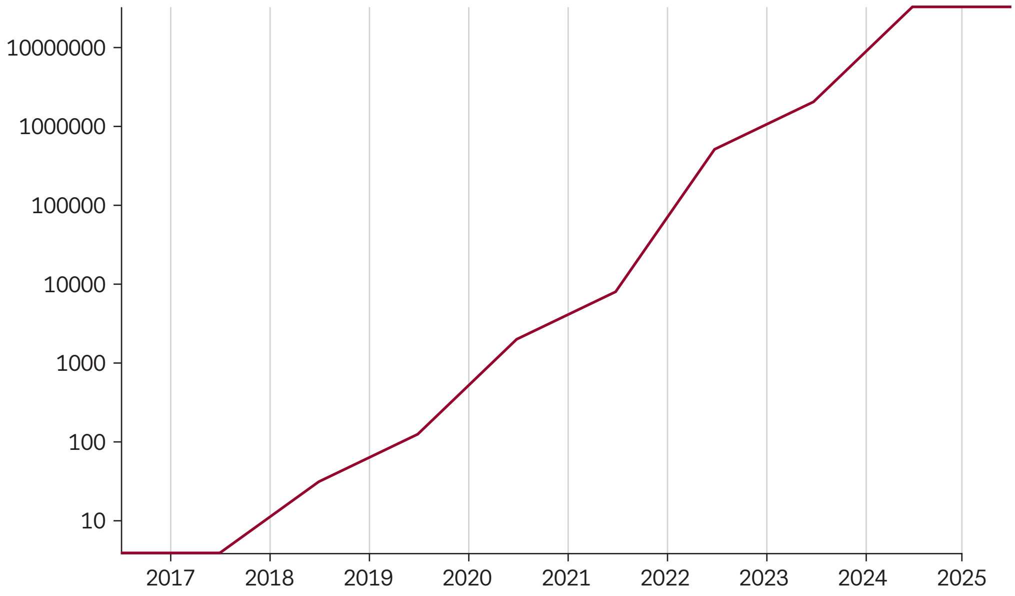
As quantum computing matures, the field has moved beyond simple qubit counts toward more nuanced performance metrics:

- Quantum volume captures a system's overall capability by accounting for qubit number, gate fidelity, connectivity, and error rates. It provides a holistic measure of computational capacity rather than raw qubit count alone.
- Circuit layer operations per second (CLOPS) measures how fast quantum systems can execute quantum circuits.
- Lambda measures how logical error rates scale as systems grow.
- Logical qubit count measures the number of error-corrected qubits a system maintains.

None of these metrics is individually determinative. A quantum computer with high-quality logical qubits, fast execution, and favorable error scaling can outperform systems with more physical qubits but poor connectivity or deteriorating error rates. The key is achieving high-enough performance across all these benchmarks.

Quantum volume—a measure of overall system performance—has improved tenfold each year since 2018 (see figure 3). In May 2025, Quantinuum achieved the new QV world record of more than eight million with a system consisting of fifty-six reliable qubits.[64] While not yet good enough for commercial use, this achievement represented a crucial turning point. It proved that quantum

FIGURE 3 Quantum volume records by year (log scale)



computers can in fact get more reliable as they get bigger.

If physical qubit counts continue to grow exponentially, overhead estimates for producing logical qubits keep falling at a similar pace, and other components of quantum volume, lambda, and CLOPS do not stagnate, the field could plausibly reach fault tolerance by the early 2030s. Of course, these are three major assumptions.

A MOORE'S LAW FOR QUANTUM?

In classical computing, the steady and predictable improvement of hardware performance followed a now-famous trajectory: Moore's law.[65] In 1965, Gordon Moore observed that the number of transistors on a chip tended to double every year. This observation became a self-fulfilling road map for innovation, investment, and policy. It enabled six decades of exponential growth in computing power and underpinned the digital revolution. The central question today is whether a quantum analog to Moore's law is emerging—and if so, what that means for commercialization, regulation, and national strategy.

From the 1930s through the 1960s, classical digital computing experimented with multiple hardware approaches—electromechanical relays, vacuum tubes, and eventually transistors—alongside new memory technologies such as magnetic drums. From decade to decade, the price-to-performance ratio of computation improved exponentially, but progress at the cutting edge moved fitfully. Many early forecasts were wildly wrong.[66]

Only after the industry began coalescing around silicon transistors did the exponential curve of Moore's law emerge. Even then, adoption lagged behind hardware capability. PCs, the internet, and smartphones were all underestimated by forecasters, who failed to grasp the implications of compounding performance and decreasing cost.

A similar fog of uncertainty surrounds quantum computing today. QC was first proposed in the 1970s, but real efforts to build hardware began only in the 1990s. There is still no scalable, error-tolerant quantum computer, and there is no equivalent of the "Bombe" code-breaking machine that catalyzed classical computing during World War II.

If progress in quantum computing were to be as rapid as in classical computation, several key measures would need to improve together at an accelerating pace:

- Quantum volume (10× annual growth since 2018)
- Logical qubit count (doubling year over year in cutting-edge systems)
- Coherence time and gate fidelity (improving steadily)
- Error-correction efficiency (dramatic declines in physical-to-logical overhead)
- Integration of control systems and cryogenics (still a bottleneck)

The co-constitutive nature of these metrics means that looking for a direct parallel to Moore's law in quantum computing is futile. For instance, improvements in error-correction code can offset lower qubit count or lower fidelity to a certain degree. At the same time, unless qubit count and fidelity improve in the longer term, better error-correction codes alone cannot achieve progress in QC. However, incorporating parallel technological improvements incrementally—one or two per generation—could sustain exponential performance growth across several metrics.

That said, the overall ecosystem is maturing fast enough to warrant immediate policy attention. Google's Willow chip showed that error-corrected qubits can outperform physical ones—and get more reliable as systems scale. DeepMind's AlphaQubit, an AI-powered error decoder, has recently demonstrated that machine learning can accelerate fault tolerance by optimizing error-correction rounds.

If these breakthroughs and others like them drive sustained exponential gains on key metrics, the compounding effects on performance and price will be enormous over longer horizons, just as they were for classical computing.

COMMERCIALIZATION PROSPECTS

If progress continues in the underlying science and engineering, the commercialization of quantum computing is likely to proceed in stages. In the near term, access will primarily be mediated through cloud-based platforms. Over the longer term, as fault-tolerant quantum computers are developed, they may deliver services predominantly via the cloud but could also justify on-premises deployment in specialized and security-sensitive settings. Below, we consider the policy implications.

HOW TO READ THE FORECASTS

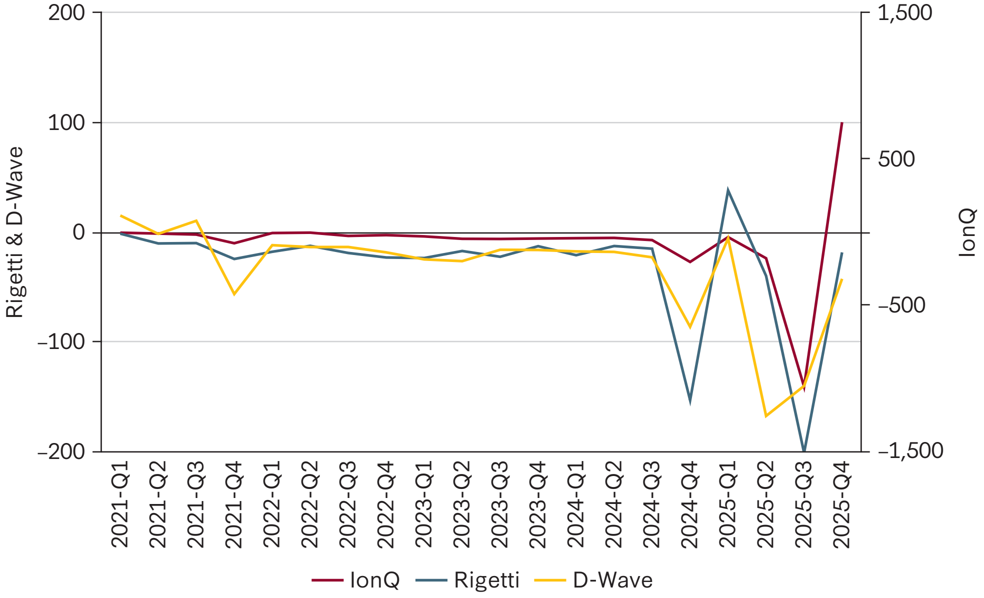
Market analysts are producing increasingly aggressive forecasts of future value creation from quantum computing. McKinsey (2024) projects that quantum computing could generate up to $2 trillion in economic value by 2035.[67] Boston Consulting Group (BCG) estimates as much as $850 billion in economic value for end users by 2040.[68] Both assume that fault-tolerant quantum computers arrive well before that point. Publicly available corporate road maps from IBM, Quantinuum, and Amazon generally converge on the early 2030s for fault tolerance (see table 2).

But the hardware may be ready before the market is. In the 1990s, the market for personal computers boomed, but it took another decade or more before highly profitable consumer and commercial internet products were developed. Creating a market for quantum-related products may require validation, regulatory approval, and market integration. It is therefore possible that the emergence of a market for quantum-derived innovations, such as new molecules, materials,

TABLE 2 COMPANY ROADMAPS

Company	Qubit modality	Milestone year	Physical qubits	Logical qubits
IBM	Superconducting	2029	NA	200
Pasqal	Neutral atoms	2029	10,000	200
PsiQuantum	Photonic	2027	1,000,000	NA
Quantinuum	Trapped ions	2029	1,000+	100+
QuEra	Neutral atoms	2026	10,000+	100
Alice & Bob	Superconducting	2030	2,000	100
IQM	Superconducting	2030	40,000	240–720

FIGURE 4 Quarterly net income of quantum computing companies, in $US millions



or batteries, may lag by many years behind the arrival of sophisticated quantum computers.

FUNDING DYNAMICS AND THE STATE OF THE INDUSTRY

In the context of a general optimism about tech, private quantum startups raised capital at a breakneck pace in 2025. Funding rounds for deep-tech firms such as PsiQuantum, Rigetti, IonQ, and QuEra have attracted hundreds of millions (billions in the case of PsiQuantum) in investment. Yet burn rates remain high, and public quantum firms have struggled since their initial public offerings (see figure 4). Both IonQ and Rigetti are heavily dependent on subsidies, partnerships, and hype-sensitive retail investment. Based on current cash burn, some firms have only two to six years of runway left without major breakthroughs or acquisitions.

Share prices remain highly vulnerable to sentiment and macro conditions. Comments from tech leaders or shifts in interest rates can move markets more than new technical milestones. This fragility raises questions about how far quantum firms will consolidate—and whether the industry's structure will begin to resemble that of semiconductors or aerospace, with a few dominant players and heavy state support. The semiconductor industry, throughout its history, has been through many boom-bust cycles. Frenzies of overinvestment have been followed by winters of overcapacity in which profits and share prices cratered.

In the near term, as discussed above, most users will access quantum computers through the cloud. QCaaS allows customers to rent time on specialized machines, lowering barriers to entry and allowing users to avoid the costs of owning and operating exotic hardware.[69] If QCaaS remains the dominant access model for firms that lack in-house quantum teams, the market dynamics will strongly favor full-stack players that can integrate hardware, software, and cloud infrastructure under one roof. This could be another driver of industry consolidation.

COSTS, SCALING, AND CLOUD LEVERAGE

QC hardware remains prohibitively expensive. Today, estimates suggest that each physical qubit in leading labs costs between $2,500[70] and $10,000.[71] A fully fault-tolerant machine could require billions of dollars in investment. Cryogenic systems, helium-3 supply chains, and control electronics add further complexity.

But, as in classical computing, cost curves will probably fall with scale. As more logical qubits become available and error correction becomes more efficient, the cost per reliable computation will drop. PsiQuantum is betting heavily on this thesis, raising over a billion dollars to build an industrial-scale computer with one million physical qubits.

AI-enhanced quantum control systems may also help drive costs down. Their advantage lies not just in capital but in vertical integration. Companies such as Google, IBM, and Quantinuum that are investing heavily in this area hope to codesign chips, error correction, cloud infrastructure, and end-user software. They also have the distribution channels and partnerships needed to commercialize at scale.

QUANTUM VS. AI, OR QUANTUM AND AI?

Rapid improvements in AI technology introduce additional, dual-sided uncertainty. AI has enabled classical computing to make surprising gains in areas once considered quantum's domain—such as search, optimization, and molecular simulation. Algorithms once thought to require a quantum advantage are now being reimagined with transformer-based architectures and differentiable programming. Additionally, the price-to-performance ratio of classical computation is falling amid massive investment in cutting-edge chips and data centers. As classical computing progresses, it may raise the bar for some use cases of quantum computing. If quantum systems are to carve out a commercial space of their own, they will eventually need to overtake AI in key use cases.

Yet AI could also speed up the development of advanced quantum computers. As we have seen, many problems remain inherently quantum in nature—including factoring large numbers or simulating entangled particles. These tasks remain out of reach for classical AI. Indeed, the two technologies are already converging, as AI could improve the entire quantum stack, from enabling better quantum error correction (e.g., AlphaQubit), to improving the design of quantum hardware, to making algorithms run more efficiently.[72] The convergence may accelerate as investors and governments realize potential synergies. However, quantum tools for AI remain largely speculative today.

STRATEGIC IMPLICATIONS

The pace of progress in quantum hardware is unmistakably exponential. QV—arguably the best composite benchmark—has improved by an order of magnitude per year for the past seven years running. Physical qubit counts and coherence times are also rising exponentially. If these trends continue, the field could cross into the fault-tolerant era by the early 2030s.

We are still far from fault-tolerant quantum computing. No current device outperforms classical systems in practical tasks. But error-corrected qubits are beginning to scale, and systems such as Google's Willow and Quantinuum's H2 suggest that the leap to utility may not be far off.

There is no dominant hardware modality. The industry still resembles classical computing in the 1950s: fragmented, exploratory, and modality diverse. Yet this also means there is room for breakthrough—and room for collapse if a modality fails to scale.

Benchmarks are improving very fast. Logical qubit overhead is falling, coherence time is rising, and QV is growing exponentially. These metrics are interdependent. Improvements in one area can unlock gains but also obscure stagnation in other areas. The lack of standardized metrics makes assessing industry progress difficult.

Commercialization will happen via the cloud first. Full-stack firms with in-house control over hardware, software, and AI integration are best positioned to benefit from early-stage demand. QCaaS will likely dominate access for years to come.

Market valuations will remain extremely volatile. If exponential trends slow, public quantum firms may face funding shortfalls. But if trends continue, the inflection point will come faster than expected—and early movers could reap vast rewards.

Part 3 examines emerging use cases in quantum sensing and communication, where quantum technologies are already showing promise in defense, navigation, and secure information transfer.

3: SENSING AND COMMUNICATIONS

Quantum sensing and quantum communications are further along the maturity curve than quantum computing and already show commercial use. QS is the near-term workhorse. It measures time, fields, motion, and gravity with exquisite sensitivity and is moving from lab systems to fieldable tools with clear dual-use impact. Military and security applications—particularly in positioning, navigation, and timing (PNT) without reliance on GPS—are a major driver of development, while commercial applications are also beginning to emerge in parallel. QComm is theoretically secure, but today's deployments are range limited, costly, and dependent on classical layers that remain attackable. The pragmatic hedge is post-quantum cryptography (PQC).

QUANTUM SENSING

WHAT IT IS AND WHY IT MATTERS

Quantum sensors use the extreme sensitivity of individual atoms to measure things such as magnetic fields, gravity, and time with precision far beyond traditional instruments. This is the oldest branch of quantum technology. First-generation systems (atomic clocks, magnetic resonance imaging [MRI], nuclear magnetic resonance [NMR]) have been in service for decades; GPS depends on atomic clocks. Second-generation sensors leverage entanglement and related effects across diverse device families. Because modern systems are sensor-reliant, improvements in sensitivity, long-term stability, size/weight/power, and cost translate quickly into real-world value.

Among the three quantum technologies, QS has the shortest path to commercialization. At high precision—up to femtoscale—QS can improve mineral exploration, medical equipment, and navigation. Critically, its significance lies not only in new markets but also in integration with existing infrastructures. For national security, this makes QS distinct. While quantum computing and quantum communications represent offensive and defensive capabilities in the digital domain, quantum sensing alters the operational landscape of existing strategic domains. Applications such as resilient navigation for submarines, detection in contested environments such as the South China Sea, and intelligence uses highlight how QS can deliver qualitatively different—and more immediate—effects on security and defense.

In short, QS is about moving decision-quality measurements out of the lab and into the field. Done right, it delivers navigation that survives spoofing and jamming, subsurface mapping that shortens surveys, and diagnostics that resolve signals glossed over by classical instruments.

USE CASES AND CURRENT EVIDENCE

Gravimetry and navigation Quantum gravimeters and gravity gradiometers resolve tiny density changes underground. Practically, that means better seismic monitoring,[73] resource discovery,[74] subsurface infrastructure mapping,[75] and space missions that can read the Earth's gravity field with finer detail.[76] Commercial systems are already deployed for geological surveys, and NASA is developing space-based quantum gradiometers for resource discovery.[77] Faster, cleaner reads of the subsurface change how we plan civil works, energy projects, and environmental monitoring.

Chemical, biological, and materials sensing Second-generation quantum sensors resolve composition and interactions at scales that challenge classical methods.[78] Portable instruments are emerging for pollution monitoring,[79] biomedical applications,[80] and industrial process control.[81] In industrial R&D, quantum microscope platforms are used for nanoscale characterization. When the measurement is the bottleneck, better sensing compresses R&D cycles and reduces waste.

Magnetometry Quantum magnetometers detect extremely weak magnetic fields with better sensitivity and size/weight/power than classical alternatives.[82] Industrialization is underway with applications in medical technology,[83] mineral exploration,[84] and battery-health monitoring.[85] Defense applications in submarine detection are real but physics-limited in range,[86] favoring bastion defense over wide-area search, and they remain far from being viable.

Positioning, navigation, and timing without GPS Quantum navigation systems combine multiple sensors—gravity detectors, magnetic field readers, rotation sensors, motion detectors, and atomic clocks—to track location and time without GPS satellites.[87] Anti-GPS attacks have risen sharply since 2018, creating economy-wide and critical-infrastructure risks.[88] Because measurements are internal, quantum PNT is jam- and spoof-resistant by design.[89] The United States is already testing prototypes of such sensors in military exercises.[90] The key hurdles to commercial and military adoption are miniaturization (reduced size, weight, power, and cost) and hardening the sensors to harsh environments (space, air, undersea).

Quantum radar / quantum illumination Quantum illumination uses quantum correlations to improve discrimination in noisy environments. Applications could include stealth detection and warhead/decoy separation.[91] However, current systems are energy intensive, require cryogenics, and face range limitations.[92] This remains a challenge for basic research.

Ecosystem and the AI link The QS market is niche and fragmented. It is dominated by university spinouts and European startups across gravimetry, precision optics, and industrial integration. AI is the force multiplier. Quantum sensors generate raw signals; AI turns the data into usable information through denoising, correlation analysis, and multisensor fusion.[93] This convergence is already showing results in biomedical scanning,[94] earthquake detection,[95] and environmental monitoring.[96]

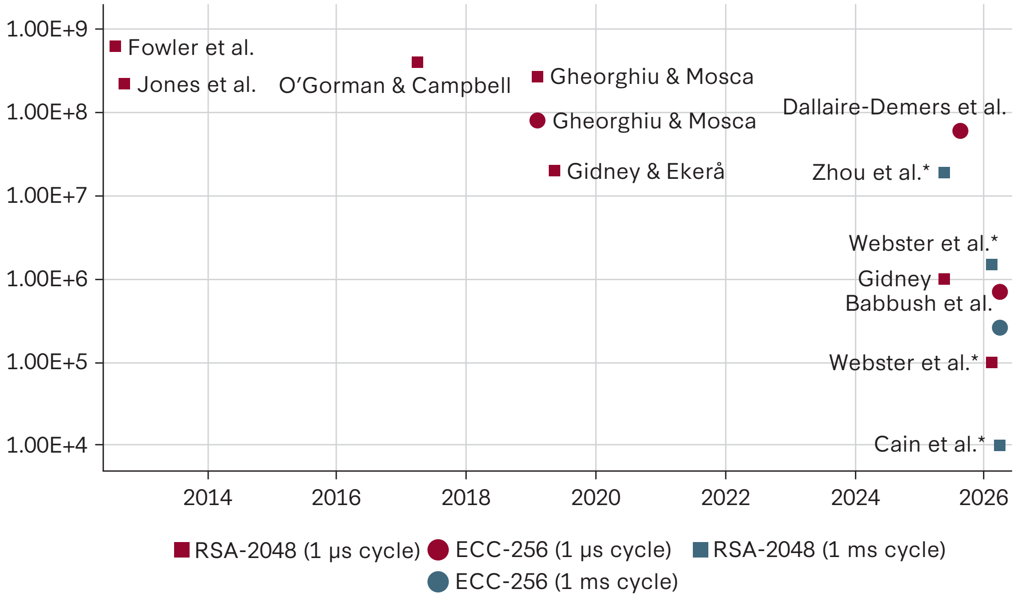
QUANTUM COMMUNICATIONS

A fault-tolerant quantum computer running Shor-class algorithms threatens RSA-2048. Resource estimates continue to drift downward (see figure 5), with some analyses suggesting fewer than one million physical qubits could factor RSA-2048 in under a week.[97] A March 2026 study estimates that this could be achieved with as few as ten thousand reconfigurable atomic qubits.[98] Forecasts vary widely, but the prudent posture is to hedge. If fast scenarios materialize, secrets encrypted today become readable tomorrow.

Quantum key distribution relies on a fundamental principle: Any attempt to intercept and read quantum information unavoidably changes it, making eavesdropping detectable—like a tamper-evident seal that cannot be resealed.[99]

But there are still significant limits to this technology.[100] Practical fiber links are short—tens to hundreds of kilometers—before loss dominates. To send quantum-secured messages over long distances, current systems use relay stations that must decrypt and reencrypt the data using traditional methods—creating vulnerable points where hackers could potentially intercept information.[101] Even in “quantum” networks, the control, authentication, and management planes remain classical and therefore vulnerable.[102] These networks are also expensive and complex to operate.

FIGURE 5 Estimated number of physical qubits to run Shor's algorithm versus year of publication



*Assume nonlocal connectivity.

Satellites extend range but introduce weather[103] and denial vulnerabilities. China's satellite demonstrations show that long-baseline quantum key distribution (QKD) is possible,[104] but so far only very small amounts of data can be transmitted.[105] Quantum repeaters could eliminate the need for trusted nodes. Implementing quantum repeaters requires neutral atom or ion systems that function essentially as small quantum computers at each relay point. But this capability remains expensive and technically demanding.[106]

The longer-run target is transmitting quantum states end to end. A true quantum network could provide complete information security with automatic intrusion detection and protect metadata.[107] It could also pool distributed quantum computing resources and enable distributed quantum sensing. However, practical networks require dependable entanglement distribution and working quantum memories. The first state to field operational end-to-end networks would gain material advantages.

In the near term, classical cryptography is the practical hedge (see table 3). Four PQC algorithms were selected in 2024–2025.[108] The US federal migration target is 2035,[109] with an estimated cost of $7 billion.[110] Longer symmetric keys provide low-cost interim hardening. Over the very long run, if end-to-end quantum networks are realized, they may be the only foolproof solution to quantum decryption. Until then, PQC is the scalable path.

STRATEGIC IMPLICATIONS

QS delivers first. Resource exploration, navigation, and scientific research are already seeing traction. On the defense side, magnetometers offer near-term capabilities but physics limits their reach, favoring defensive applications. Quantum PNT represents a credible path to jam- and spoof-resistant navigation.

In QComm, broad impact depends on end-to-end quantum networks; near-term activity will remain limited to specialized pilots while PQC drives real

TABLE 3 PQC VS. QKD

	PQC	QKD
Advantages	Software deployable; hardware agnostic; designed to resist classical and quantum attacks; fits existing networks.	Detects eavesdropping on key exchange in principle; true quantum network could provide complete information security.
Drawbacks	Requires widespread migration across networks.	Today's deployments are short-range and rely on trusted nodes; classical surfaces remain attack-able; satellites extend range but add weather/ denial constraints; current systems have limited applicability.
Operational picture	Deploy PQC broadly.	Keep QKD specialized until repeater-class capabilities mature.

migration. If fast quantum-computing scenarios materialize, then cryptographic timelines will compress, making all three quantum domains strategically urgent. States will need to deploy PQC rapidly, introduce QS pilots where they reduce operational risks, and sustain research on the technologies that enable true quantum networks.

4: GEOPOLITICS

The global quantum ecosystem is multipolar. While the United States and China are the two largest national players, the European Union as a whole is close behind (see figure 6). The UK, Japan, Australia, Canada, and other countries also have robust quantum ecosystems, including university labs, talent, and componentry manufacturers.

To generalize, leadership is split by domain. The United States leads in QC. China is meaningfully ahead in QComm. QS leadership is distributed across the US, Europe, and China. That distribution shows up in top-cited papers, in developer ecosystems, and in the staffs of standards bodies.

The US quantum ecosystem is undoubtedly deep. Private capital, cloud access, and developer programs are strengths. IBM reports five hundred thousand–plus users on its platform.[111] Federal cryptography planning centers on PQC with a government migration target in 2035.[112] Current-generation QKD remains specialized and bounded by trusted nodes and classical control planes.

Yet no country, even the United States, is remotely self-sufficient. Europe and Japan anchor production of critical components—dilution refrigerators, lasers/optics, single-photon detectors, cryoelectronics. Supply chains are shallow and geographically diffuse. The US and allies have tightened access for People’s Republic of China (PRC) entities. China, meanwhile, is actively pursuing domestic substitution policies to achieve self-reliance across quantum supply chains.

STRATEGIC CONTEXT

Quantum technologies map onto core state functions. QC affects cryptographic resilience and accelerates simulation and optimization for energy, materials, logistics, and defense. QComm aims at eavesdrop-resistant links, though today’s deployments rely on trusted nodes and depend on classical authentication and control systems, as well as free-space links that remain weather and denial prone. QS pushes precision in timekeeping, field sensing, and inertial navigation, enabling jam/spoof-resistant PNT, subsurface mapping, and intelligence, surveillance, and reconnaissance (ISR)–adjacent missions.

All three domains are dual-use and remain precommercial in broad terms. That makes the competition geopolitical first, commercial second.

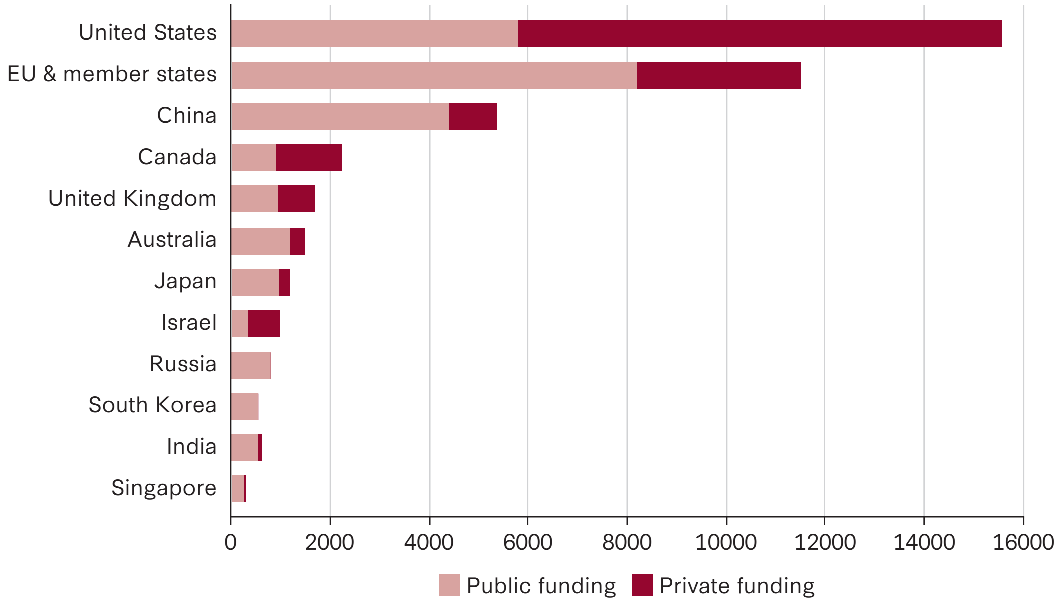
NATIONAL APPROACHES

UNITED STATES

The United States operates an ecosystem-first model under the National Quantum Initiative (NQI), with the US National Institute of Standards and Technology (NIST), the National Science Foundation (NSF), the Department of Energy (DOE), the Department of War (DoW), and NASA sharing responsibility.[113] The private sector is broad and deep, offering cloud access through Amazon Web Services (AWS), Azure, and Google, alongside open software development kits (SDKs) and large communities of developers.

In quantum computing, US and allied vendors lead many public benchmarks. Open-access programs and reproducible metrics have reinforced a Western-oriented developer stack, with third-party labs and national facilities providing validation. The approach emphasizes breadth of institutions, depth of private capital, and the scale of developer access that IBM’s five hundred thousand–plus figure represents.

FIGURE 6 Estimated public and private funding for quantum technologies, in $US millions, 2020 to February 2025, including planned investments



Federal cryptography planning centers on post-quantum cryptography, with a 2035 migration target for government systems.[114] Current-generation QKD is not used for internal government communications as it is costly, complex to implement, and vulnerable to attack.[115]

The United States hosts around twenty companies developing quantum sensors at the cutting edge, many of which receive Defense Advanced Research Projects Agency (DARPA) funding. The US military has started testing quantum sensors for PNT in military exercises. However, the US lead in QS has narrowed considerably since 2022.[116]

CHINA

China's approach is state directed and security led, based on an assumption that quantum technologies could have "transformative" industrial and geopolitical implications.[117] Quantum decryption is a key concern. Peng Chengzhi, chief quantum scientist at China Telecom, has noted that advancing QC poses "severe challenges to information security."[118] China's quantum investments have been most concentrated in long-haul QKD fiber, satellite QKD, and a small number of university-anchored hubs, notably Hefei. Corporate quantum labs at large tech firms have been folded into state universities, signaling consolidation around centralized research centers.[119]

China has built the largest terrestrial QKD networks and demonstrated long-baseline satellite links.[120] The government,[121] the military, and the financial sector[122] are reported users. A commercial system integrating QKD with PQC was announced in 2025.[123] QKD's practical use and security remain disputed today, as many architectures still lean on trusted nodes and classical control planes that remain vulnerable. China leads in deployment scale. However, comparisons to allied capabilities are complicated because many allied agencies have deprioritized QKD for general-purpose use in favor of PQC.

In quantum computing, public signals are mixed relative to US/UK/EU vendors. In 2020, Pan Jianwei, China's most prominent quantum scientist, asserted that "China as a whole stands on a level playing field with developed nations" in quantum computing.[124] Chinese universities have posted notable demonstrations, with Tsinghua University teams boasting that they are among the world's best.[125] However, vendor-grade systems trail Western leaders on several open metrics.[126] Publication and patent volume is high, though incentives and domestic citation density make raw counts noisy indicators of actual capability.[127] Some notable Chinese tech companies, including Baidu, have also scaled back investments in QC.[128]

China's QS research extends across clocks, magnetometry, and cold-atom systems. There is less public evidence of China deploying QS in the field than QComm. According to Pan, China "still lags behind developed nations to some extent" in QS but is advancing rapidly.[129] QS is clearly a priority, since it fits into China's stated priorities for defense modernization.[130]

In conclusion, China's overall strategy appears to hedge multiple approaches: deploy QKD where feasible; pursue PQC in parallel; build indigenous supply chains for cryogenics, optics, and detectors; and concentrate talent and equipment in a few state-backed hubs.[131]

ALLIES AND PARTNERS

Allied countries (EU, UK, Japan, Australia, and Canada) have national programs, university spinouts, and companies that lead or remain competitive in key functions across the quantum ecosystem. Europe and Japan anchor component depth across dilution refrigerators, high-power/low-noise lasers, precision optics, single-photon detectors, and cryoelectronics.[132] The UK and EU are home to leading QS firms and test beds. Japan's optics and laser ecosystem is pivotal across all quantum modalities. European vendors lead in several subdomains of QC.[133] There have been several QKD pilots across Europe and Japan. Europe leads in several forms of QS, as we have seen, including commercial cold-atom gravimetry and gravity-gradiometry lineages. The UK and EU have visible defense-relevant navigation trials, and Australia is a key partner for quantum-enabled PNT. Allied governments also have strong representation in international quantum standard-setting bodies. They therefore have significant influence over emerging technical norms.

RESEARCH LANDSCAPE

Patterns in the most-cited quantum scientific literature broadly align with these visible deployment patterns. Bluntly stated, the US leads in QC, China leads in QComm, and QS leadership is split among the US, the EU, and China.

China has overtaken the US in total STEM publications,[134] but evaluating the quality of these publications is more challenging, as even leading Chinese scientists admit (see figure 7).[135] China's government offers incentives for scientists to publish.[136] It has historically rewarded sheer volume of publications, high-impact placements, and high-density citation of other PRC scholars.[137] Retraction data for PRC scientists are well above global averages.[138] For quantum specifically, the best signal of China's research strength is its scholars' representation in top quantum journals (see figures 8–10).

Patent data are similarly hard to parse. PRC scientists apply for more patents; US scientists are more likely to win them.[139] Leading Western patent holders include IBM, Google, D-Wave, and Microsoft.[140] Patent charts indicate intent and investment levels but are not direct measures of technical performance or commercial viability.

What is clear from maps of global research collaboration networks is that US-China cooperation on quantum is deep and wide-ranging across QC, QComm, and QS.[141] As Washington grows more skeptical of research cooperation, China's labs are shifting toward collaborations with other leading countries. This transition matters for replication quality, shared datasets, and access to

FIGURE 7 Nature Index Adjusted Share metric for publications in science journals (in thousands)

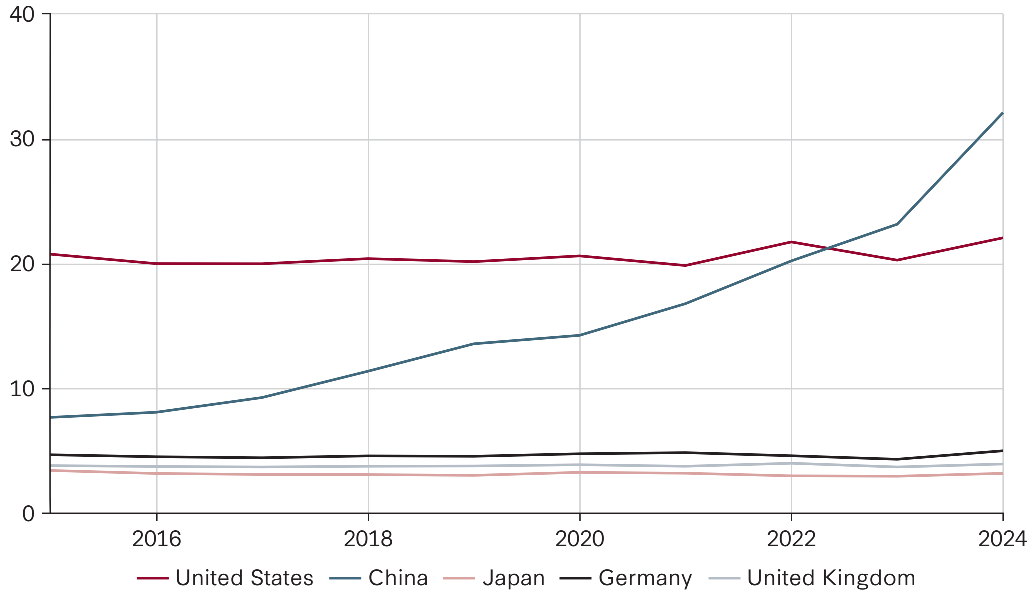
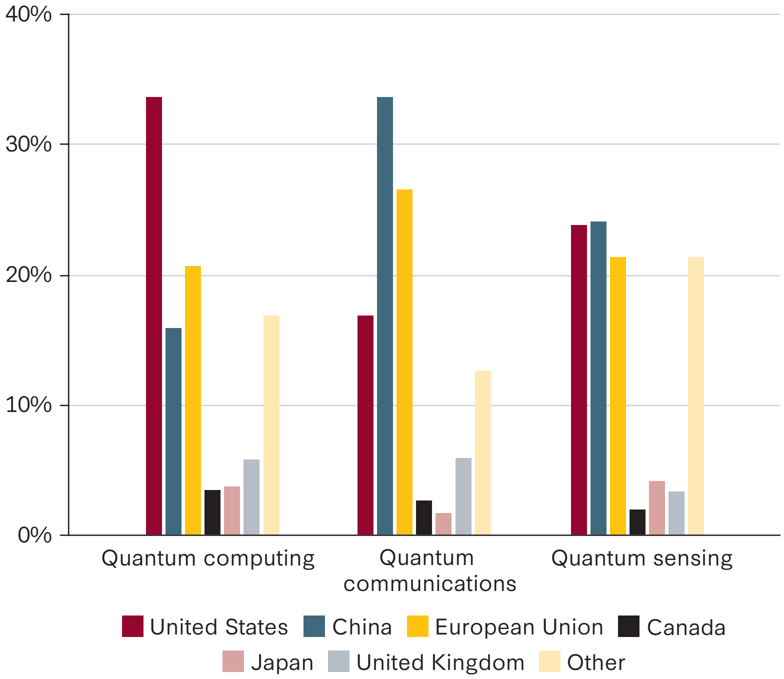


FIGURE 8 Share of top 10 percent most-cited papers by country/region, 2019–2023



specialized hardware. It may advantage the labs of US allies over US labs. It may also improve China's ability to extract Western intellectual property—and create hidden networks of dependency within Western quantum supply chains.

PRIVATE-SECTOR AND CAPITAL MARKETS

The market for quantum products and services is highly geographically diverse (see table 4). The EU

FIGURE 9 Share of quantum computing publications by region (2019–2023)

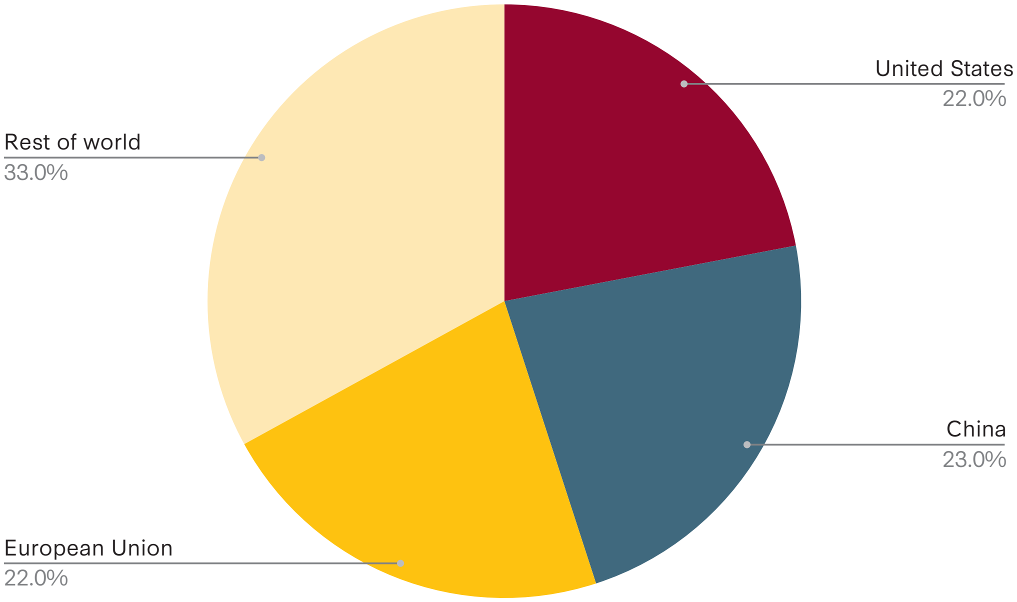
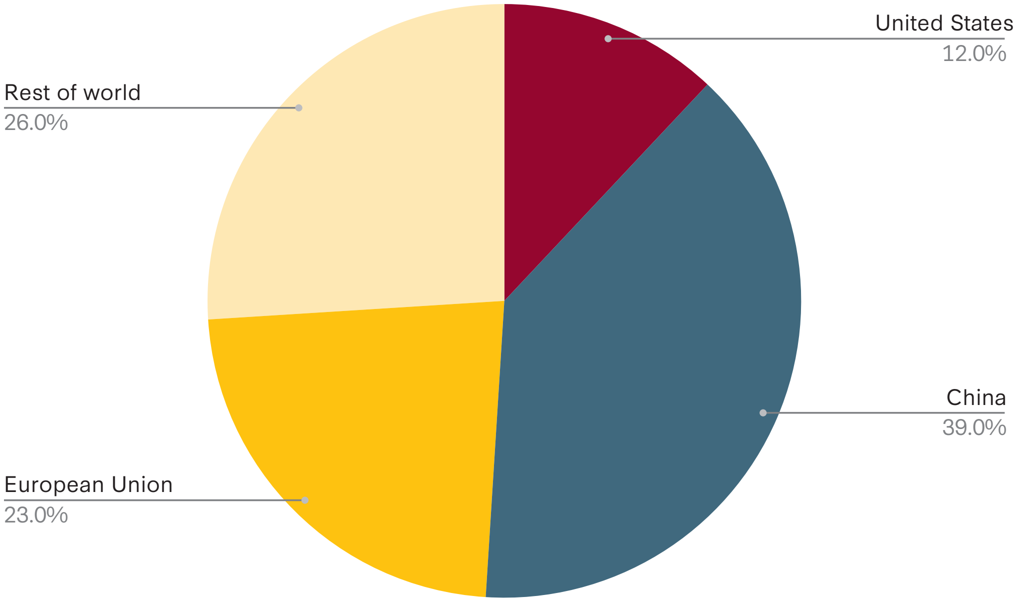


FIGURE 10 Share of quantum communications publications by region (2019–2023)



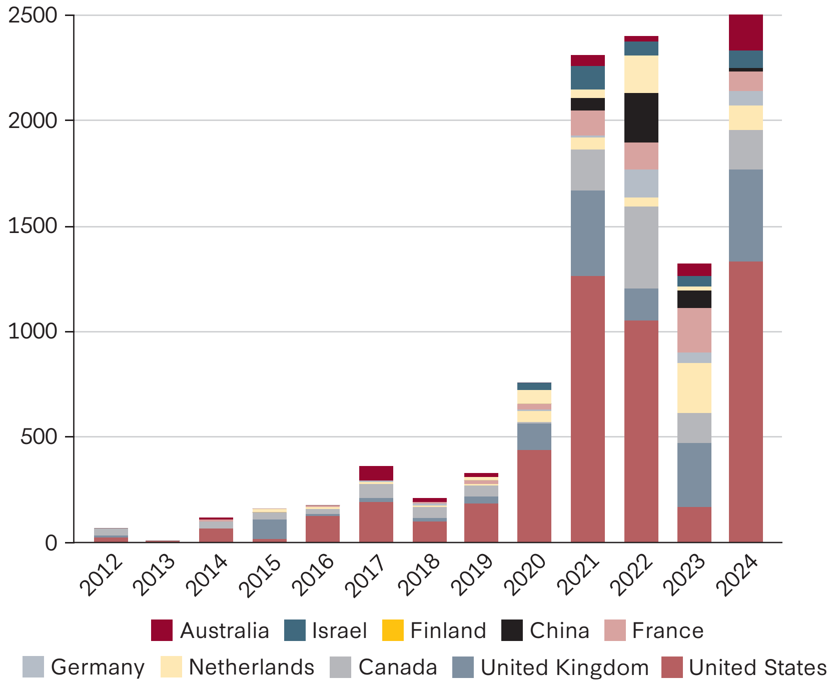
hosts the largest cluster of pure-play quantum firms. These include hardware startups, full-stack vendors, and control-electronics and software companies. The United States follows closely behind in the number of pure-play quantum companies.[142] The UK, Canada, Germany, and France all have sizable company counts and visible university spinout pipelines. China's private sector has a smaller footprint in quantum. Most cutting-edge quantum research in China appears to take place in state laboratories and a handful of universities, despite efforts by leading scholars to cooperate with private firms.[143]

The picture grows even more complex when one considers the funding structure. The US quantum ecosystem depends heavily on venture capital

TABLE 4 QUANTUM TECHNOLOGY PURE-PLAY JOB OPENINGS AND WORKERS BY REGION, 2024

Region	Openings	Workers
Europe and Central Asia	1,341	7,366
North America	1,089	5,551
East Asia and Pacific	139	828
Middle East and North Africa	60	491
South Asia	18	264
Latin America and Caribbean	1	17

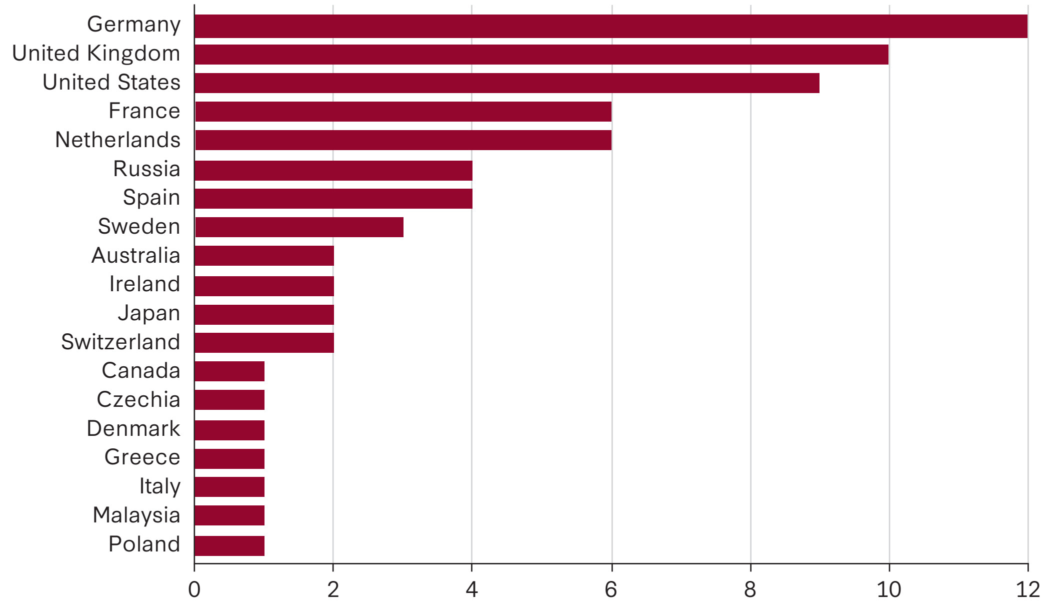
FIGURE 11 Venture funding for quantum technology companies, in $US millions



funding (see figure 11). In boom times this can be a blessing, though it raises risks if market sentiment sours. Europe's venture base is thinner, but government-backed research programs and national labs help bridge funding gaps. Much of Europe's best quantum research happens within universities. In China, state-directed funds[144] and municipal programs underwrite university labs and selected vendors.[145] State-owned telecom companies such as China Telecom have also invested in QComm.

Even within countries, leading quantum companies are highly geographically distributed. For classical computing, leading companies are overwhelmingly headquartered in Silicon Valley, with a few exceptions in Seattle. Cities such as New York and Austin serve as secondary hubs. By contrast, the North American quantum scene has hubs in the Chicago-Midwest corridor, Boston-Cambridge, Silicon Valley, Boulder-Denver, the Maryland-DC belt, New York, Los Angeles, and the Waterloo-Toronto

FIGURE 12 Number of master's degrees with "quantum" in the degree title, by country/region (2024)



and Vancouver corridors.[146] In Europe, there are major supplier and lab ecosystems in Zurich, Munich, Paris-Saclay, the Delft-Leiden-Amsterdam triangle, Oxford-Cambridge, Bristol-London, Vienna-Innsbruck, Helsinki-Espoo, and Berlin-Potsdam. In China, capability is notably concentrated in Hefei.

There are several reasons for this broader geographic dispersion. Quantum research grew out of university physics departments and national labs worldwide, rather than from a single commercial breakthrough that created clustering effects as the semiconductor industry did in California. Most countries with advanced research capabilities have national quantum programs, spreading talent across many locations. Exotic hardware requirements mean specialized suppliers developed wherever there was existing expertise. Finally, unlike software/internet companies that can locate anywhere, quantum research requires expensive lab infrastructure that is anchored to established universities and national research facilities.

TALENT DYNAMICS

The United States benefits from the scale and diversity of its STEM base plus private-sector career paths. Yet the US quantum ecosystem is highly dependent on foreign-born talent.[147]

China's specialist pool has historically been smaller.[148] The quality spread is wide: A few flagship groups perform at the frontier while many labs remain at an earlier stage. Concentration in Hefei and select hubs accelerates training but creates single-point exposure to disruption. China's leading quantum experts are keenly aware of these problems.[149] Beijing has signaled a determination to improve the breadth and depth of the nation's quantum talent pool.[150]

Europe trains and employs a large, steady flow of quantum-relevant graduates and hosts more than forty specialized master's programs (see figure 12).[151] The UK, Japan, Australia, and Canada operate top laboratories in atomic, molecular, and optical (AMO) physics, photonics, and control electronics. The allied system serves as the natural destination for coadvised degrees, shared facilities, and developer-to-research pipelines.

The global quantum talent pool is small and highly mobile. The center of gravity within subfields can shift quickly with visa rules, grant flows, export controls, and other incentives. Today, US immigration and student visa policies drive away talent. For example, International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) are two sets of US export-control laws that restrict firms working on US government contracts from hiring certain (or any) foreign nationals. If US visa regulations grow even more restrictive, it is entirely possible that the next generation of promising quantum startups will originate in countries such as Singapore and Switzerland.[152]

STANDARD-SETTING

Standards development is another underappreciated area of geopolitical competition. A critical lesson from classical computing history is that sustainable dominance requires vertical integration of the entire technology stack. NVIDIA has achieved a dominant position in advanced graphics processing unit chips (GPUs) partly because the developer ecosystem is locked into its proprietary CUDA application programming interface. Leadership in quantum computing will ultimately require excellence beyond the physical qubit layer, including in error correction firmware, control software, programming languages, and application frameworks.

US companies are currently well-positioned. The Microsoft-backed QIR initiative is becoming the de facto intermediate representation standard.[153] US cloud providers are hoping to apply this lesson by integrating quantum services into existing infrastructure. China's strategy of massive state-directed hardware investment may therefore achieve technical parity or even temporary superiority in specific metrics—but it could also fail because China's ecosystem of developer tools, programming frameworks, cloud platforms, and industry partnerships falls behind. This is a key reason why standard-setting matters.

Standard-setting for PQC is relatively far advanced. The US government's timeline for PQC sets expectations for vendors, integrators, and public agencies globally. The quantum computing industry is beginning to agree on common programming languages and standards that allow different types of quantum hardware and software to work together.

Standards for QComm and QS are more fragmented. QKD protocols and implementations span fiber and free-space approaches with different authentication layers and key-management schemes. Sensing standards remain in an early stage. Metrology bodies and national labs define traceability and calibration for their own clocks, gravimeters, magnetometers, and inertial systems. Commercial lineages in gravimetry and diamond-based microscopy are pushing interoperability and data-format conventions from the bottom up. Defense and space programs add environmental and ruggedization specifications that filter back to civilian suppliers. There are various international working groups trying to advance these standards, but they are not yet far along.

THE ALGORITHM PROBLEM AND ALLIED STRATEGY

A distinctive feature of quantum computing is that the field's ultimate strategic significance depends on algorithmic discoveries that have not yet been made. If the algorithm problem remains largely unsolved, even fault-tolerant machines may have limited impact outside quantum simulation and cryptography. But if US researchers identify new algorithms with exponential speedups that apply to commercially or militarily significant problems, China and US-allied countries could suddenly find themselves in a sprint to scale up the necessary hardware.

This uncertainty has important implications for allied coordination. Most likely, algorithmic discoveries will diffuse rapidly. The quantum algorithm research community is small, internationally networked, and rooted in academic norms of open publication. Attempting to classify algorithmic breakthroughs would require a dramatic shift in research culture and would likely fail regardless because the relevant researchers are globally mobile. The realistic assumption is that any significant algorithmic breakthrough becomes globally known within months to years.

However, the likely speed of diffusion is not symmetrical. If China achieves an algorithmic breakthrough in a military-backed lab, its discovery is more likely to be kept secret than if the same breakthrough takes place at Stanford or Cambridge. Even when results are published, diffusion can also take time. The scientists and engineers who discover new techniques often have tacit knowledge about how to implement, optimize, and apply their ideas. This unwritten knowledge can take more time to transfer than headline findings.

The allies' best strategy is therefore to maximize the chances that breakthroughs happen inside allied institutions first, and prepare to respond with decisive and coordinated state support when necessary. This is yet another reason to coordinate policy on talent retention, visa policy, and funding for basic research at universities and national labs.

Precisely because algorithmic breakthroughs are likely to diffuse as global public knowledge, the most durable sources of strategic leverage lie elsewhere: in hardware supply chains, platform standards, and the geographic distribution of enabling technologies. Allied coordination should focus on areas where advantage can be sustained. China is hedging in ways that suggest Beijing understands this logic. Today, all quantum computing progress globally is bottlenecked by the shortage of effective algorithms. China is building out quantum hardware infrastructure now to position itself to exploit any algorithmic breakthrough faster than its competitors—whether that breakthrough emerges from domestic labs, from open scientific literature, or from a foreign lab that China can target with espionage.

SUPPLY CHAINS AND CONTROLS

Quantum hardware depends on shallow, geographically concentrated supply chains. Ultracold refrigerators are essential for most quantum computers. Specialized light detectors enable quantum communication and sensing. High-precision lasers control trapped ion and neutral atom systems. Without these components, progress stops. Additional critical parts include amplifiers that work at extreme cold, control chips designed for cryogenic operation, and specialized manufacturing tools. Many of these components come from just a handful of suppliers worldwide.[154] Between single-source suppliers, long lead times, and specialized service requirements, the quantum ecosystem faces extraordinary vulnerabilities.

Geography concentrates risk and opportunity. Europe and Japan anchor many component categories, notably optical and photonic components, single-photon detection, and cryogenic infrastructure. The United States overlaps several of these categories, too, in addition to quantum control and error correction, some substrate materials, and system integration. China excels in low-cost commercial electronics and optics but has historically depended on US-allied suppliers for several quantum-specific components. It is the dominant processor of some substrate materials, such as niobium. Israel is among the leading producers of control electronics. Unlike the artificial intelligence supply chain, quantum hardware is more geographically distributed, there are significantly more players as modalities are not standardized, and supply chains are shallow (see table 5).

The general trend is toward tightening export controls. US measures have added Chinese quantum entities to restricted lists.[155] Coordination with allies has increased, with security partnerships identifying quantum technologies—especially PNT—for joint experimentation.[156] Within allied circles, early measures to ease dual-use collaboration coexist with tighter controls on sensitive subsystems.[157] Announcements have generally outpaced joint funding and shared deliverables, while component geography continues to determine practical outcomes. However, given that

TABLE 5 QUANTUM HARDWARE COMPONENTS SUPPLY CHAIN

Select components	Use	Key suppliers
Quantum control and error correction		
ASICs/FPGAs for real-time decoding	Low-latency decoding of error syndromes and feedback control so correction keeps up with cycle time	Riverlane (Cambridge, UK); AMD/Xilinx (San Jose, US); Altera (Santa Clara, US)
Quantum control & readout electronics	Generating/routing control pulses and acquiring readout signals; synchronizing timing; supporting feedback loops	Quantum Machines (Tel Aviv, Israel); Zurich Instruments (Zurich, Switzerland); Qblox (Delft, Netherlands)
Precision lasers	Narrow-line-width, frequency-stabilized lasers for cooling, trapping, and gates	TOPTICA Photonics (Gräfelfing, Germany); NKT Photonics (Birkerød, Denmark); Coherent (Santa Clara, US); Precilasers (Shanghai, China)
Laser diodes	Semiconductor laser diodes for cooling/trapping, pumping, and control wavelengths	Nichia (Anan, Japan); ams OSRAM (Regensburg, Germany); TOPTICA Photonics (Gräfelfing, Germany)
Cryogenic microwave low-noise amplifiers	Amplifying weak microwave readout signals at cryogenic stages with minimal added noise	Low Noise Factory (Gothenburg, Sweden); QuinStar (Torrance, US)
Optical and photonic components		
Spatial light modulators (SLMs)	Shaping laser beams to trap and address individual atom qubits	Hamamatsu Photonics (Hamamatsu City, Japan); HOLOEYE Photonics (Berlin, Germany); Meadowlark Optics (Frederick, US)
Electro-optic modulators (EOMs)	Fast phase/intensity/polarization modulation for laser-based qubit control	Thorlabs (Newton, US); Exail (Saint-Germain-en-Laye, France); EOSPACE (Redmond, US); QUBIG GmbH (Munich, Germany)
Acousto-optic devices (AOMs/AODs)	Fast frequency shifting, switching, and beam deflection for atom/ion operations	Gooch & Housego (Ilminster, UK); Brimrose (Sparks, US); AA Opto-Electronic (Orsay, France); Isomet (Manassas, US)

TABLE 5 (*Continued*)

Select components	Use	Key suppliers
Nanophotonics	Subwavelength photonic circuits	imec (Leuven, Belgium); SMART Photonics (Eindhoven, Netherlands); LIGENTEC (Switzerland/France); AIM Photonics (Albany, US)
Single-photon detection		
Superconducting nanowire single-photon detectors (SNSPDs)	Cryogenic single-photon detection	ID Quantique (Geneva, Switzerland); Photon Spot (Monrovia, US); Single Quantum (Delft, Netherlands)
Electron-multiplying charge-coupled devices (EMCCDs)	Low-light imaging for trapped ion/neutral atom fluorescence readout	Teledyne Princeton Instruments (Trenton, US); Nüvü Camēras (Montreal, Canada); Oxford Instruments (Abingdon, UK)
Single-photon counting modules (SPCMs) and avalanche diodes (SPADs)	Compact photon counting; sometimes array readout	Excelitas (Waltham, US); Hamamatsu (Hamamatsu City, Japan); Photon Force (Edinburgh, UK)
Cryogenic and vacuum infrastructure		
Dilution refrigerators	Cooling quantum processors to <20 mK	Bluefors (Helsinki, Finland); Quantum Design (San Diego, US); FormFactor (Livermore, US); Leiden Cryogenics (Leiden, Netherlands)
Cryocoolers and compressors	Precooling stages (3–4 K) and cryocooler infrastructure	SHI Cryogenics (Japan/US); Bluefors (Helsinki, Finland)
Ultra-high vacuum (UHV) chambers	Vacuum enclosures isolating trapped ions and neutral atoms	ULVAC (Chigasaki, Japan); Kurt J. Lesker (Jefferson Hills, US); Kimball Physics (Wilton, US)
Fabrication equipment		
Lithography tools	Optical and e-beam nanopatterning of quantum processor chips	ASML (Veldhoven, Netherlands); Canon (Tokyo, Japan); Raith (Dortmund, Germany); JEOL (Tokyo, Japan)
Substrate and strategic materials		
Sapphire substrates	Low-loss substrates for superconducting circuits	Crystal Systems (Salem, US); Kyocera (Kyoto, Japan); Rubicon Technology (Bensenville, US)
Isotopically enriched silicon-28	Nuclear-spin-free silicon to extend coherence of spin qubits	ASP Isotopes (Washington, DC, US; enrichment facilities in South Africa); Urenco Stable Isotopes (Almelo, Netherlands)
Niobium	Superconducting material used in resonators, in cavities, and as targets for deposition	CBMM (Araxá, Brazil); Niobec/Magris (Saint-Honoré, Canada); Chinese processors
Helium-3	Active cooling medium in dilution refrigerators	DOE Isotope Program (US); Linde (global); Air Liquide (Paris, France)

quantum hardware supply chains remain highly diffuse and immature, current restrictions on technology transfer will do little to stifle Chinese advances. Having learned its lesson from the race in artificial intelligence, China is responding by making quantum self-sufficiency a national priority.

The overall picture is of an emerging industry with obvious dual-use significance that is dependent on brittle and poorly mapped supply chains.

CONCLUSION

We are still in the early days of quantum technology. The physics is established for quantum computing, sensing, and communications. But the engineering is still being worked out for each, and the clocks are not necessarily synchronized.

We have taken a historical perspective in this report because policymakers must understand how quantum differs fundamentally from classical computing. Given the blazing progress on key benchmarks of quantum computing, it is tempting to draw analogies to Moore's law and classical computing—tempting, but incorrect. Classical computing improved steadily along one path: smaller, faster chips. Quantum computing needs multiple technologies to advance simultaneously: better qubits, improved error correction, and sophisticated control systems.

The need for continued progress along multiple dimensions makes the timeline for quantum commercialization harder to predict. Classical computing has run on silicon for three-quarters of a century, but quantum remains fragmented across superconducting circuits, neutral atoms, trapped ions, electron spins, and photonics—with no clear winner. Quantum requires exotic infrastructure from day one. Because of the diverse hardware and software tools involved, and the ambiguity of key metrics, tracking the horse race in quantum is not straightforward. Unlike with classical computing in the 1960s, the quantum stack is hardware heavy from the start and dual-use by default.

The development pattern also differs in several ways. First, standards: In classical computing, standards emerged after mass markets developed. In quantum, technical norms are hardening around laboratory interoperability before any consumer applications exist. Second, uncertainty about use cases: We remain fundamentally uncertain about what problems quantum computers will ultimately be able to solve. The shortage of useful algorithms is distinct from the engineering challenge of scaling up fault-tolerant quantum computers. It is another reason for allied governments to focus on supporting basic research, not just hardware supply chains. Third, "harvest-now, decrypt-later" dynamics: Encrypted data stolen today could become readable retroactively once quantum computers mature. This risk raises the stakes of the competition to develop large-scale QC first.

Surveying the field in historical perspective, four main themes stand out about emerging technical trends:

1. *Feedback loops are reinforcing.* The three main quantum technology groups are distinct, but they are not completely siloed. All three domains rely upon highly coherent quantum systems and sophisticated classical control hardware. This technological overlap means that advances in any one domain can accelerate progress in the others, creating compounding benefits from sustained investment across the full quantum ecosystem.
2. *Technical bottlenecks are shared across domains.* Today, control electronics constrain progress across all three quantum technology groups. Improvements in certain components could benefit the entire stack.

3. *Platforms and settings matter.* Cloud-based quantum access is already shaping developer adoption patterns and technical standards. Platform choices made today will influence technical standards and alliance structures, shaping the competitive ecosystem for years or decades.

4. *AI and quantum are converging.* AI and quantum computing are in a sense competing to perform certain functions. With AI improving rapidly, the bar is rising for quantum computers to stand on their own as viable commercial products. However, from a long-term perspective, the two technologies have immense potential for synergy.

On the geopolitical level, we draw three main conclusions:

1. *No one nation will control the full stack.* The United States is strong in computing platforms and developer ecosystems. China leads in large-scale QKD deployments. Europe and Japan lead in production of key components, including refrigerators, precision lasers, and single-photon detectors. As quantum technology becomes more geopolitically significant, the US will need help from allies to build out and sustain its quantum technology ecosystem. There is an intrinsic tension between this goal, the need to protect dual-use technologies, and allies' desire for tech sovereignty.

2. *There are bottlenecks in hardware and software.* Many critical parts come from a handful of allied suppliers. Lead times for some parts are long and variable. Control hardware is growing more sophisticated and embedded with software. In this context, the lesson of semiconductors is that progress toward fault-tolerant quantum computing may depend as much on secure access to dilution refrigerators as on qubit physics. The US and allied governments must start taking supply chain risks seriously, starting by mapping bottlenecks in China.

3. *Integrated research networks remain the center of gravity.* Quantum is coming of age in the era of cloud computing. The global research ecosystem is highly connected and geographically dispersed, with top labs, talent, and components spanning the US, Europe, Japan, Canada, Australia, China, and other nations. Multipolarity is a structural feature of the ecosystem. Thus, despite the United States' advantages in its startup ecosystem and capital market, it is not currently prepared to dictate or dominate the quantum ecosystem as it does in AI.

Ultimately, the race for quantum advantage will not be defined by a single breakthrough but by the ability to sustain innovation across this diffuse, multipolar landscape. For US policymakers, the task is not to replicate a closed, vertical model of dominance but to orchestrate a resilient alliance network that can weather technical uncertainty.

APPENDIX: A GUIDE TO LEADING QUBIT MODALITIES

Quantum computers encode information in qubits, the quantum equivalent of the classical bit. Unlike classical bits, which are always either 0 or 1, qubits can exist in combinations of both states simultaneously—a property called superposition. Several fundamentally different physical systems can serve as qubits, each with distinct advantages and limitations. This appendix summarizes the leading approaches.

A note on cooling: Nearly all quantum computers require extreme environmental control to protect fragile quantum states from thermal noise. Some modalities use cryogenic refrigeration (dilution refrigerators that reach temperatures colder than outer space), while others use precision laser techniques to slow atoms to near motionlessness. These are very different engineering requirements with different costs and infrastructure implications, even though both achieve “cold” qubits. The distinctions are noted for each modality below.

SUPERCONDUCTING QUBITS

Status: Most mature and widely deployed modality

Key players: Google, IBM, Rigetti, IQM, Qolab, QuantWare, Nord Quantique, Oxford Quantum Circuits

Superconducting qubits use electrical circuits made from materials that conduct electricity with zero resistance when cooled to extreme temperatures. They are fabricated using techniques adapted from the semiconductor industry, making them relatively straightforward to manufacture. Within this category, transmon qubits dominate. Quantum gate operations on superconducting qubits are very fast—typically completing in tens of nanoseconds—and the control techniques are well understood after more than two decades of development.

The principal limitation is that these qubits lose their quantum information quickly (short coherence times), which means computations must be completed rapidly or protected by error correction. They also require dilution refrigerators that cool the processor to approximately 15 millikelvin—roughly two hundred times colder than outer space—which creates significant infrastructure requirements. Scaling beyond a few hundred qubits remains challenging due to wiring density, the physical size and cooling requirements of refrigeration systems, and the overhead of quantum error correction.

CAT QUBITS

Status: Early stage; promising but unproven at scale

Key players: Alice & Bob, AWS

Cat qubits are a specialized type of superconducting qubit—they use the same cryogenic platform and fabrication ecosystem. The name comes from Schrödinger’s cat, the famous thought experiment about quantum uncertainty, because these qubits store information in electromagnetic field states that simultaneously occupy two distinct configurations.

Their key innovation is that they are engineered so that one of the two main types of quantum error (bit-flip errors) is exponentially suppressed by design. This means that error correction only needs to handle the remaining error type (phase-flip errors), which could dramatically reduce the number of physical qubits needed per logical qubit—potentially by an order of magnitude compared to standard superconducting approaches. However, cat qubits are at an earlier stage of development than conventional transmon qubits, and significant fabrication and engineering challenges remain before this theoretical advantage can be realized in practice.

SPIN QUBITS

Status: Mid-stage research; strong long-term manufacturing case

Key players: Intel, CEA-Leti, Quantum Motion, Diraq, Groove Quantum, Quobly, Silicon Quantum Computing

Spin qubits encode quantum information in the magnetic spin of individual electrons trapped in semiconductor structures. Their most compelling advantage for policymakers is compatibility with existing complementary metal oxide semiconductor (CMOS) manufacturing—the same industrial processes used to make classical computer chips. If spin qubits can be made to work reliably, they could potentially be produced at scale in existing fabrication facilities, dramatically reducing production costs and enabling very-high-density qubit arrays. Each qubit is also extremely small, on the order of tens of nanometers.

Spin qubits operate at cryogenic temperatures, typically in the range of tens of millikelvin to around 1 Kelvin depending on the specific implementation—cold, but some variants operate at significantly warmer temperatures than superconducting qubits. The main challenges are that individual electron spins are extremely delicate and difficult to control precisely, coherence times are relatively short, and achieving reliable two-qubit operations remains an active area of research.

TRAPPED ION QUBITS

Status: Mature; highest demonstrated gate fidelities

Key players: IonQ, Quantinuum, Universal Quantum

Trapped ion systems use individual charged atoms (ions) suspended in a vacuum by electromagnetic fields. The ions are cooled to near their quantum ground state using precisely tuned lasers—a fundamentally different cooling mechanism from the dilution refrigerators used by superconducting and spin qubits. Some implementations do use cryogenic vacuum chambers to improve vacuum quality and reduce interference from background gas molecules, but the qubit cooling itself is achieved optically.

Trapped ions offer the longest coherence times and the lowest error rates of any current qubit technology, making them a strong platform for near-term demonstrations of quantum advantage. The principal trade-off is speed: Gate operations are significantly slower than in superconducting systems, typically taking microseconds rather than nanoseconds. Scaling is also challenging. As the number of ions in a single trap increases, controlling their collective motion becomes progressively harder. Most current architectures experience performance degradation beyond roughly fifty to one hundred ions, though modular approaches that shuttle ions between connected trap zones are being developed to overcome this limit.

NEUTRAL ATOM QUBITS

Status: Rapidly advancing; strong scalability demonstrations

Key players: QuEra, Pasqal, Atom Computing, Infleqtion, Google

Neutral atom qubits use uncharged atoms held in place by tightly focused laser beams (known as optical tweezers) and manipulated via their electronic states. Like trapped ions, they are laser cooled rather than cryogenically refrigerated, which simplifies some infrastructure requirements. Quantum interactions between atoms are induced by briefly exciting them to high-energy “Rydberg states,” allowing programmable, long-range connections between qubits.

This modality offers particularly promising scalability. Current systems have demonstrated arrays of several hundred atoms—already competitive with the largest superconducting processors—and the architecture naturally supports dense two- and three-dimensional arrangements. The principal trade-off is gate speed, which is slower than superconducting systems, and achieving uniformly high-fidelity operations across large arrays remains an active engineering challenge.

PHOTONIC QUBITS

Status: Mid-stage research; unique architectural advantages, major technical hurdles

Key players: Xanadu, PsiQuantum, Orca

Photonic quantum computers encode information in individual particles of light (photons). They are attractive because they can operate at or near room temperature and could potentially integrate with existing fiber-optic telecommunications infrastructure, offering a natural pathway to networked quantum computing.

The core challenge is that photons do not naturally interact with each other, which makes two-qubit gate operations—essential for universal quantum computation—extremely difficult to implement reliably. Current approaches rely on measurement-based schemes that are inherently probabilistic, meaning gates only succeed a fraction of the time. Reliable single-photon generation and detection at the rates required for computation also remain significant engineering obstacles. However, if these challenges can be overcome, photonic systems could offer distinctive advantages in networking and modularity.

TOPOLOGICAL QUBITS

Status: Earliest stage; potentially transformative but experimentally unproven

Key players: Microsoft

Topological qubits aim to encode quantum information in collective properties of exotic quantum states that are inherently protected from local disturbances—much as a knot in a rope cannot be undone by jostling the middle of the rope. This built-in protection could make them far more resistant to errors than any other qubit type, potentially reducing the overhead of quantum error correction by orders of magnitude.

Microsoft announced progress in 2025 with a chip based on Majorana-type particles, shifting the conversation from purely theoretical to early experimental demonstrations. However, the scientific community remains divided on timelines, and the gap between demonstrating the underlying physics and building a working, scalable quantum computer using this approach is substantial. If the approach succeeds, it could be transformative; the risk is that it may take significantly longer than competing modalities to reach practical utility.

ACKNOWLEDGMENTS

The authors are grateful to Stephen Kotkin and Niall Ferguson for securing the funding that made this report possible; to Jon Simon, Dave Schuster, and Amir Safavi-Naeini for their detailed peer review; to Cheryl Steets and Martin Giles; and to the Hoover Publishing team.

FIGURE AND TABLE SOURCES

FIGURES

Figure 1: Rami Barends, Alireza Shabani, Lucas Lamata, et al., "Digitized Adiabatic Quantum Computing with a Superconducting Circuit," *Nature* 534, no. 7606 (June 8, 2016): 222–26, https://doi.org/10.1038/nature17658; "IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation," IBM Newsroom, May 4, 2016, https://uk.newsroom.ibm.com/2016-May-04-IBM-Makes-Quantum-Computing-Available-on-IBM-Cloud-to-Accelerate-Innovation; Hamish Johnston, "IBM Offers 20-Qubit Quantum Computer to Clients," *Physics World*, November 15, 2017, https://physicsworld.com/a/ibm-offers-20-qubit-quantum-computer-to-clients/; "IBM Unveils Breakthrough 127-Qubit Quantum Processor," IBM Newsroom, November 16, 2021, https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor; "IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two," IBM Newsroom, November 9, 2022, https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two; Jay Gambetta, "The Hardware and Software for the Era of Quantum Utility Is Here," *IBM Quantum Blog*, December 4, 2023, https://www.ibm.com/quantum/blog/quantum-roadmap-2033; John Martinis and Sergio Boixo, "Quantum Supremacy Using a Programmable Superconducting Processor," *Google Research Blog*, October 23, 2019, https://research.google/blog/quantum-supremacy-using-a-programmable-superconducting-processor/; Hartmut Neven, "Meet Willow, Our State-of-the-Art Quantum Chip," *The Keyword*, December 10, 2024, https://blog.google/innovation-and-ai/technology/research/google-willow-quantum-chip/; Brian Wang, "Rigetti Scalable Universal Quantum Qubits and Launching of 36 Simulated Qubit Cloud," NextBigFuture, August 5, 2017, https://www.nextbigfuture.com/2017/08/rigetti-scalable-universal-quantum-qubits-and-launching-of-36-simulated-qubit-cloud.html; Michael Feldman, "Quantum Computing Startup Takes on Tech Giants," Top500, August 13, 2018, https://www.top500.org/news/quantum-computing-startup-takes-on-tech-giants/; *January 2022 Investor Presentation*, Rigetti Computing, January 2022, https://www.rigetti.com/uploads/January-2022-Investor-Presentation.pdf; "Rigetti Computing Announces Commercial Availability of 80-Qubit Aspen-M System and Results of CLOPS Speed Tests," Rigetti Investors, February 15, 2022, https://investors.rigetti.com/news-releases/news-release-details/rigetti-computing-announces-commercial-availability-80-qubit; "Rigetti Computing Launches 84-Qubit Ankaa™-3 System; Achieves 99.5% Median 2-Qubit Gate Fidelity Milestone," Rigetti Investors, December 23, 2024, https://investors.rigetti.com/news-releases/news-release-details/rigetti-computing-launches-84-qubit-ankaatm-3-system-achieves; Mohib Ur Rehman, "Rigetti Announces General Availability of 108-Qubit System," *The Quantum Insider*, April 8, 2026, https://thequantuminsider.com/2026/04/08/rigetti-108-qubit-system-availability/; "Quantinuum Completes Hardware Upgrade; Achieves 20 Fully Connected Qubits," Quantinuum, June 14, 2022, https://www.quantinuum.com/press-releases/quantinuum-completes-hardware-upgrade-achieves-20-fully-connected-qubits; Ilyas Khan, "Quantinuum and Microsoft Achieve Breakthrough That Unlocks a New Era of Reliable Quantum Computing," *Quantinuum Blog*, April 3, 2024, https://www.quantinuum.com/blog/a-new-breakthrough-in-logical-quantum-computing-reveals-the-scale-of-our-industry-leadership; "Quantinuum Launches Industry-First, Trapped-Ion 56-Qubit Quantum Computer, Breaking Key Benchmark Record," Quantinuum, June 5, 2024, https://www.quantinuum.com/press-releases/quantinuum-launches-industry-first-trapped-ion-56-qubit-quantum-computer-that-challenges-the-worlds-best-supercomputers; "Introducing Helios: The Most Accurate Quantum Computer in the World," *Quantinuum Blog*, November 5, 2025, https://www.quantinuum.com/blog/introducing-helios-the-most-accurate-quantum-computer-in-the-world; and Matt Swayne, "Quantum Startup Atom Computing First to Exceed 1,000 Qubits," *The Quantum Insider*, June 17, 2024, https://thequantuminsider.com/2023/10/24/quantum-startup-atom-computing-first-to-exceed-1000-qubits/.

Figure 2: Dave Kielpinski, V. Meyer, M. A. Rowe, et al., "A Decoherence-Free Quantum Memory Using Trapped Ions," *Science* 291, no. 5506 (February 9, 2001): 1013–15, https://doi.org/10.1126/science.1057357; John M. Martinis, S. Nam, J. Aumentado, and C. Urbina, "Rabi Oscillations in a Large Josephson-Junction Qubit," *Physical Review Letters* 89, no. 11 (August 21, 2002), https://doi.org/10.1103/PhysRevLett.89.117901;

C. Langer, R. Ozeri, J. D. Jost, et al., "Long-Lived Qubit Memory Using Atomic Ions," *Physical Review Letters* 95, no. 6 (August 2, 2005), https://doi.org/10.1103/PhysRevLett.95.060502; J. A. Schreier, A. A. Houck, Jens Koch, et al., "Suppressing Charge Noise Decoherence in Superconducting Charge Qubits," arXiv:0712.3581 (2007), https://doi.org/10.48550/arxiv.0712.3581; Matthias Steffen, "Superconducting Qubits Are Getting Serious," *Physics* 4 (December 2011), https://doi.org/10.1103/Physics.4.103; Waseem S. Bakr, Philipp M. Preiss, M. Eric Tai, Ruichao Ma, Jonathan Simon, and Markus Greiner, "Orbital Excitation Blockade and Algorithmic Cooling in Quantum Gases," *Nature* 480, no. 7378 (December 22, 2011): 500–503, https://doi.org/10.1038/nature10668; Arvind Mamgain, Siddhi Satish Khaire, Ujjawal Singhal, et al., "A Review of Developments in Superconducting Quantum Processors," *Journal of the Indian Institute of Science* 103, no. 2 (October 2023): 633–69, https://doi.org/10.1007/s41745-022-00330-z; Jungsang Kim, "Trapped Ions Make Impeccable Qubits," *Physics* 7, no. 119 (November 2014), https://doi.org/10.1103/Physics.7.119; Jiaheng Yang, Xiaodong He, Ruijun Guo, et al., "Coherence Preservation of a Single Neutral Atom Qubit Transferred Between Magic-Intensity Optical Traps," *Physical Review Letters* 117, no. 12 (September 14, 2016), https://doi.org/10.1103/PhysRevLett.117.123201; Ye Wang, Mark Um, Junhua Zhang et al., "Single-Qubit Quantum Memory Exceeding Ten-Minute Coherence Time," *Nature Photonics* 11 (September 25, 2017): 646–50, https://doi.org/10.1038/s41566-017-0007-1; Mark Saffman, "Quantum Computing with Neutral Atoms," *National Science Review* 6, no.1 (September 10, 2019), https://doi.org/10.1093/nsr/nwy088; Morten Kjaergaard, Mollie E. Schwartz, Jochen Braumüller, et al., "Superconducting Qubits: Current State of Play," *Annual Review of Condensed Matter Physics* 11, (March 2020): 369–95, https://doi.org/10.1146/annurev-conmatphys-031119-050605; Alexander P. M. Place, Lila V. H. Rodgers, Pranav Mundada, et al., "New Material Platform for Superconducting Transmon Qubits with Coherence Times Exceeding 0.3 Milliseconds," *Nature Communications* 12 (March 19, 2021), https://doi.org/10.1038/s41467-021-22030-5; Pengfei Wang, Chun-Yang Luan, Mu Qiao, et al., "Single Ion Qubit with Estimated Coherence Time Exceeding One Hour," *Nature Communications* 12, no. 1 (January 11, 2021), https://doi.org/10.1038/s41467-020-20330-w; Steven M. Girvin, "Extending Superconducting Qubit Lifetimes: What's Next?," *Journal Club for Condensed Matter Physics* (September 2021), https://www.osti.gov/servlets/purl/1866115; Paul Smith-Goodson, "Atom Computing Sets a World Record Coherence Time for Neutral Atom Qubits," *Forbes*, June 2, 2022, https://www.forbes.com/sites/moorinsights/2022/06/02/atom-computing-sets-a-world-record-coherence-time-for-neutral-atom-qubits/; Aaron Somoroff, Quentin Ficheux, Raymond A. Mencia, et al., "Millisecond Coherence in a Superconducting Qubit," *Physical Review Letters* 130, no. 26 (June 29, 2023), https://doi.org/10.1103/PhysRevLett.130.267001; Matthew P. Bland, Faranak Bahrami, Jeronimo G. C. Martinez, et al., "Millisecond Lifetimes and Coherence Times in 2D Transmon Qubits," *Nature* 647 (November 5, 2025): 343–48, https://doi.org/10.1038/s41586-025-09687-4; Jiahao Pi et al., "Beyond-Ten-Hour Coherence in a Decoherence-Free Trapped-Ion Clock Qubit," arXiv:2603.19631 (2026), https://doi.org/10.48550/arxiv.2603.19631; and D. Mishin, D. Tregubov, N. Kolachevsky, and A. Golovizin, "Coherence of Microwave and Optical Qubit Levels in Neutral Thulium," *PRX Quantum* 6, no. 4 (November 10, 2025), https://doi.org/10.1103/f8xg-w57m.

Figure 3: Paul Smith-Goodson, "IBM Doubles Its Quantum Computing Power Again," *Forbes*, January 8, 2020, https://www.forbes.com/sites/moorinsights/2020/01/08/ibm-doubles-its-quantum-computing-power-again/; Stephen Shankland, "IBM Doubles Its Quantum Computer Performance," CNET, August 20, 2020, https://www.cnet.com/tech/computing/ibm-doubles-its-quantum-computer-performance/; "Achieving Quantum Volume 128 on the Honeywell Quantum Computer," Honeywell, accessed May 11, 2026, https://www.honeywell.com/us/en/news/2020/09/achieving-quantum-volume-128-on-the-honeywell-quantum-computer; "Demonstrating Benefits of Quantum Upgradable Design Strategy: System Model H1-2 First to Prove 2,048 Quantum Volume," *Quantinuum Blog*, December 29, 2021, https://www.quantinuum.com/blog/demonstrating-benefits-of-quantum-upgradable-design-strategy-system-model-h1-2-first-to-prove-2-048-quantum-volume; Matt Swayne "Quantinuum Marks Record in Quantum Volume, New Capabilities and Rising Subscribers," *The Quantum Insider*, April 21, 2024, https://thequantuminsider.com/2022/09/27/quantinuum-marks-record-in-quantum-volume-new-capabilities-and-rising-subscribers/; Matt Swayne, "Quantinuum H-Series Quantum Computer Registers Three More Quantum Volume Performance Records," *The Quantum Insider*, April 20, 2024, https://thequantuminsider.com/2023/07/03/quantinuum-h-series-quantum-computer-registers-three-more-quantum-volume-performance-records/; "System Model H2 Series," Quantinuum, accessed May 11, 2026, https://www.quantinuum.com/products-solutions/system-model-h2-series; and "Quantum Volume," Quantinuum, accessed May 11, 2026, https://www.quantinuum.com/glossary-item/quantum-volume.

Figure 4: Quarterly net income/loss data compiled by authors from IonQ Inc., Rigetti Computing Inc., and D-Wave Quantum Inc. Forms 10-Q and 10-K filed with the US Securities and Exchange Commission, 2021–2025.

Figure 5: Author estimates based on Ryan Babbush, Adam Zalcman, Craig Gidney, et al., "Securing Elliptic Curve Cryptocurrencies Against Quantum Vulnerabilities: Resource Estimates and Mitigations," arXiv:2603.28846 (2026); Madelyn Cain, Qian Xu, Robbie King, et al., "Shor's Algorithm Is Possible with as Few as 10,000 Reconfigurable Atomic Qubits," arXiv:2603.28627 (2026); Pierre-Luc Dallaire-Demers, William Doyle, and Timothy Foo, "Brace for Impact: ECDLP Challenges for Quantum Cryptanalysis," arXiv:2508.14011 (2025); Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland, "Surface Codes: Towards Practical Large-Scale Quantum Computation," *Physical Review A* 86, no. 3 (2012): 032324, https://doi.org/10.1103/PhysRevA.86.032324; Vlad Gheorghiu and Michele Mosca, "Benchmarking the Quantum Cryptanalysis of Symmetric, Public-Key and Hash-Based Cryptographic Schemes," arXiv:1902.02332 (2019); Craig Gidney, "How to Factor 2048 Bit RSA Integers with Less Than a Million Noisy Qubits," arXiv:2505.15917 (2025); Craig Gidney and Martin Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," *Quantum* 5 (2021): 433, https://doi.org/10.22331/q-2021-04-15-433; N. Cody Jones, Rodney Van Meter, Austin G. Fowler, et al., "Layered Architecture for Quantum Computing," *Physical Review X* 2, no. 3 (2012): 031007, https://doi.org/10.1103/PhysRevX.2.031007; Joe O'Gorman and Earl T. Campbell, "Quantum Computation with Realistic Magic-State Factories," *Physical Review A* 95, no. 3 (2017): 032338, https://doi.org/10.1103/PhysRevA.95.032338; Paul Webster, Lucas Berent, Omprakash Chandra, et al., "The Pinnacle Architecture: Reducing the Cost of Breaking RSA-2048 to 100,000 Physical Qubits Using Quantum LDPC Codes," arXiv:2602.11457 (2026); Hengyun Zhou, Casey Duckering, Chen Zhao, et al., "Resource Analysis of Low-Overhead Transversal Architectures for Reconfigurable Atom Arrays," in *Proceedings of the 52nd Annual International Symposium on Computer Architecture (ISCA '25)* (ACM, 2025), https://doi.org/10.1145/3695053.3731039.

Figure 6: Author estimates based on own research and Olivier Ezratty, *Understanding Quantum Technologies 2025* (independently published, 2025), https://www.oezratty.net/wordpress/2025/understanding-quantum-technologies-2025/.

Figure 7: Nature Index, "Country/Territory Rankings," Springer Nature, https://www.nature.com/nature-index/country-outputs/generate/all/global.

Figure 8: "Critical Technology Tracker," Australian Strategic Policy Institute (2025), https://techtracker.aspi.org.au/tech/quantum-communication/research-contribution/.

Figures 9–12: Jonathan Ruane, Elif Kiesow, Johannes Galatsanos, Carl Dukatz, Edward Blomquist, and Prashant Shukla, *Quantum Index Report 2025* (MIT Initiative on the Digital Economy, 2025), https://qir.mit.edu/wp-content/uploads/2025/06/MIT-QIR-2025.pdf.

TABLES

Table 2: Ryan Mandelbaum, Jay Gambetta, Jerry Chow, et al., "How IBM Will Build the World's First Large-Scale, Fault-Tolerant Quantum Computer," *IBM Quantum Blog*, June 10, 2025, https://www.ibm.com/quantum/blog/large-scale-ftqc; "Our Roadmap," Pasqal, accessed April 10, 2026, https://www.pasqal.com/technology/roadmap; Alex Mack, "PsiQuantum to Build World's First Utility-Scale, Fault-Tolerant Quantum Computer in Australia," PsiQuantum, April 29, 2024, https://www.psiquantum.com/news-import/psiquantum-to-build-worlds-first-utility-scale-fault-tolerant-quantum-computer-in-australia; Doug Finke, "Quantinuum Announces Its Processor Development Roadmap," Quantum Computing Report, July 4, 2025, https://quantumcomputingreport.com/quantinuum-announces-its-processor-development-roadmap/; "QuEra Computing Releases a Groundbreaking Roadmap for Advanced Error-Corrected Quantum Computers, Pioneering the Next Frontier in Quantum Innovation," QuEra, January 9, 2024, https://www.quera.com/press-releases/quera-computing-releases-a-groundbreaking-roadmap-for-advanced-error-corrected-quantum-computers-pioneering-the-next-frontier-in-quantum-innovation-0; Raphaël Lescanne, "Alice & Bob 2030 Roadmap to Useful Quantum Computers: Our Bet in Quantum Computing," *Alice & Bob*, accessed October 5, 2025, https://alice-bob.com/blog/alice-bob-2030-roadmap-to-useful-quantum-computers/; and "Development Roadmap," IQM, accessed October 5, 2025, https://meetiqm.com/technology/roadmap/.

Table 4: Elliott J. Mason, "State of Quantum Industry Innovation—What Patents Tell Us," QED-C, December 11, 2024, https://quantumconsortium.org/publication/state-of-quantum-industry-innovation-what-patents-tell-us/.

Table 5: Olivier Ezratty, *Understanding Quantum Technologies 2024* (independently published, 2024), accessed October 6, 2025, https://www.oezratty.net/wordpress/2024/understanding-quantum-technologies-2024/.

NOTES

1. 深圳卫视财经频道, “专访潘建伟：2035年中国有望造出谷通用量子计算机” [Interview with Pan Jianwei: China is expected to build a universal quantum computer by 2035], 未来科学大奖 [Future Science Prize], July 16, 2025, https://www.futureprize.org/cn/nav/detail/1731.html.

2. Craig Gidney, “How to Factor 2048 Bit RSA Integers with Less Than a Million Noisy Qubits,” arXiv, May 21, 2025, https://arxiv.org/abs/2505.15917; and “IQM Quantum Computers Unveils Development Roadmap Focused on Fault-Tolerant Quantum Computing by 2030,” IQM Quantum Computers, November 13, 2024, https://meetiqm.com/press-releases/iqm-quantum-computers-unveils-development-roadmap-focused-on-fault-tolerant-quantum-computing-by-2030/.

3. Fredrik Erixon, Andrea Dugo, Dyuti Pandya, and Oscar du Roy, “Benchmarking Quantum Technology Performance: Governments, Industry, Academia and Their Role in Shaping Our Technological Future,” Policy Brief 06/2025 (ECIPE, 2025), https://ecipe.org/wp-content/uploads/2025/03/ECI_25_PolicyBrief_06-2025_LY03.pdf.

4. Elizabeth Gibney, “Mini-Satellite Paves the Way for Quantum Messaging Anywhere on Earth,” *Nature*, March 19, 2025, https://doi.org/10.1038/d41586-025-00581-7. More details in Chinese: 中国科学院空间主动光电技术重点实验室, “‘墨子号’量子卫星首次洲际量子密钥分发细节” [“Micius” quantum satellite conducts first intercontinental quantum key distribution], 中国科学院空间主动光电技术重点实验室 [Key Laboratory of Space Active Optical-Electro Technology, Chinese Academy of Sciences], January 29, 2018, http://www.sitp.cas.cn/kjzdgdsys/xwtz/xwdt/202010/t20201013_5715770.html.

5. Alexander Miller, “Micius, the World’s First Quantum Communication Satellite, Was Hackable,” arXiv, May 10, 2025, https://arxiv.org/abs/2505.06532.

6. Dongxin Gao, Daojin Fan, Chen Zha, et al., “Establishing a New Benchmark in Quantum Computational Advantage with 105-Qubit Zuchongzhi 3.0 Processor,” *Physical Review Letters* 134, no. 9 (March 3, 2025): 090601, https://doi.org/10.1103/physrevlett.134.090601.

7. Vlatko Vedral, “Quantum Information—the Basics,” in *Introduction to Quantum Information Science* (Oxford University Press, 2006), chap. 3, https://academic.oup.com/book/8602/chapter-abstract/154543238?redirectedFrom=fulltext.

8. Fabio Sciarrino, Francesco de Martini, Stuart R. Hameroff, and Yi Zeng, “Quantum Superposition,” ScienceDirect, accessed October 7, 2025, https://www.sciencedirect.com/topics/engineering/quantum-superposition.

9. Vlatko Vedral, “Quantum Entanglement—Introduction,” in *Introduction to Quantum Information Science*, chap. 7, https://academic.oup.com/book/8602/chapter-abstract/154560283?redirectedFrom=fulltext; and “What Is Entanglement and Why Is It Important?,” Caltech Science Exchange, accessed October 7, 2025, https://scienceexchange.caltech.edu/topics/quantum-science-explained/entanglement.

10. Vlatko Vedral, “Quantum Entanglement in Practice,” in *Introduction to Quantum Information Science*, chap. 9, https://academic.oup.com/book/8602/chapter-abstract/154570627?redirectedFrom=fulltext.

11. Vlatko Vedral, “Measure of Entanglement,” in *Introduction to Quantum Information Science*, chap. 10, https://academic.oup.com/book/8602/chapter-abstract/154571698?redirectedFrom=fulltext; and Vlatko Vedral, “Classical Information,” in *Introduction to Quantum Information Science*, chap. 1, https://academic.oup.com/book/8602/chapter-abstract/154529650?redirectedFrom=fulltext.

12. Jared D. Weidman, Manas Sajjan, Camille Mikolas et al., “Quantum Computing and Chemistry,” *Cell Reports Physical Science* 9, no. 9 (September 18, 2024): 102105, https://doi.org/10.1016/j.xcrp.2024.102105; Arunima Singh, “Chemical Space Exploration with Quantum Computing,” *Nature Methods* 22, no. 3 (March 12, 2025): 452, https://doi.org/10.1038/s41592-025-02638-x; Davide Castelvecchi, “Single Particle Acts as a Quantum Computer to Simulate Molecules,” *Nature*, May 16, 2025, https://doi.org/10.1038/d41586-025-01591-1; and Weitang Li, Zhi Yin, Xiaoran Li, et al., “A Hybrid Quantum Computing Pipeline for Real World Drug Discovery,” *Scientific Reports* 14, no. 1 (July 23, 2024), https://doi.org/10.1038/s41598-024-67897-8.

13. Sören Wilkening, Andreea-Iulia Lefterovici, Lennart Binkowski, Michael Perk, Sándor P. Fekete, and Tobias J. Osborne, “A Quantum Algorithm for Solving 0-1 Knapsack Problems,” *npj Quantum Information* 11 (2025): 146, https://www.nature.com/articles/s41534-025-01097-8; and Giuseppe Buonaiuto, Francesco Gargiulo, Giuseppe De Pietro, Massimo Esposito, and Marco Pota, “Best Practices for Portfolio Optimization by Quantum Computing, Experimented on Real Quantum Devices,” *Scientific Reports* 13 (2023): 19434, https://doi.org/10.1038/s41598-023-45392-w.

14. Muhammad AbuGhanem, “Characterizing Grover Search Algorithm on Large-Scale Superconducting Quantum Computers,” *Scientific Reports* 15 (2025): 1281, https://doi.org/10.1038/s41598-024-80188-6; and Yifan Sun and Lian-Ao Wu, “Quantum Search Algorithm on Weighted Databases,” *Scientific Reports* 14 (2024): 30169, https://doi.org/10.1038/s41598-024-81701-7.

15. Jingwen Ding, Giuseppe Spallitta, and Roberto Sebastiani, “Effective Prime Factorization via Quantum Annealing by Modular Locally-Structured Embedding,” *Scientific Reports* 14 (2024): 3518, https://doi.org/10.1038

/s41598-024-53708-7; and Michele Mosca, Joao Marcos Vensi Basso, and Sebastian R. Verschoor, "On Speeding Up Factoring with Quantum SAT Solvers," *Scientific Reports* 10, no. 1 (September 14, 2020), https://doi.org/10.1038/s41598-020-71654-y.

16. Kyungtaek Jun and Hyunju Lee, "HUBO and QUBO Models for Prime Factorization," *Scientific Reports* 13 (2023): 10080, https://doi.org/10.1038/s41598-023-36813-x.

17. Alexander Nico-Katz, Nathan Keenan, and John Goold, "Can Quantum Computers Do Nothing?," *npj Quantum Information* 10 (2024): 124, https://doi.org/10.1038/s41534-024-00918-6; and Vlatko Vedral, "Quantum Error Correction," in *Introduction to Quantum Information Science*, chap. 13, https://academic.oup.com/book/8602/chapter-abstract/154589645?redirectedFrom=fulltext.

18. Matthew Parker, "Controlling Qubits with Cryogenic Devices," *Nature Electronics* 5 (March 29, 2022), https://doi.org/10.1038/s41928-022-00740-y.

19. Parker, "Controlling Qubits."

20. Hans Gundlach, Keeper Sharkey, Jayson Lynch, et al., "Quantum Advantage in Computational Chemistry?," arXiv, August 28, 2025, https://arxiv.org/abs/2508.20972; Markus Reiher, Nathan Wiebe, Krysta M. Svore, and Matthias Troyer, "Elucidating Reaction Mechanisms on Quantum Computers," *Proceedings of the National Academy of Sciences* 114, no. 29 (July 3, 2017): 7555–60, https://doi.org/10.1073/pnas.1619152114; and Jakob Günther, Freek Witteveen, Alexander Schmidhuber, Marek Miller, Matthias Christandl, and Aram Harrow, "Phase Estimation with Partially Randomized Time Evolution," arXiv, March 7, 2025, https://arxiv.org/abs/2503.05647.

21. Richard P. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics* 21, nos. 6/7 (1982), https://s2.smu.edu/~mitch/class/5395/papers/feynman-quantum-1981.pdf.

22. Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, 1994), 124–34, https://doi.org/10.1109/SFCS.1994.365700.

23. Davide Castelvecchi, "The Race to Save the Internet from Quantum Hackers," *Nature* 602 (February 8, 2022), https://doi.org/10.1038/d41586-022-00339-5; and Marcos Allende, Diego López León, Sergio Cerón, et al., "Quantum-Resistance in Blockchain Networks," *Nature Scientific Reports* 13 (April 6, 2023), https://doi.org/10.1038/s41598-023-32701-6.

24. Paul Webster, Lucas Berent, Omprakash Chandra, et al., "The Pinnacle Architecture: Reducing the Cost of Breaking RSA-2048 to 100,000 Physical Qubits Using Quantum LDPC Codes," arXiv, February 12, 2026, https://doi.org/10.48550/arXiv.2602.11457.

25. Chad Boutin, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," NIST, August 13, 2024, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

26. Herb Lin, "A Retrospective Post-Quantum Policy Problem," *Lawfare*, September 14, 2022, https://www.lawfaremedia.org/article/retrospective-post-quantum-policy-problem.

27. Lov K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," arXiv, May 29, 1996, https://arxiv.org/abs/quant-ph/9605043.

28. C. Lavor, L. R. U. Manssur, and R. Portugal, "Grover's Algorithm: Quantum Database Search," arXiv, January 16, 2003, https://arxiv.org/abs/quant-ph/0301079.

29. Hassen Nigatu, Shi Gaokun, Li Jituo, Wang Jin, Lu Guodong, and Howard Li, "Quantum Machine Learning and Grover's Algorithm for Quantum Optimization of Robotic Manipulators," arXiv, September 8, 2025, https://arxiv.org/abs/2509.07216.

30. Buonaiuto et al., "Best Practices for Portfolio Optimization"; and Kamila Zaman, Alberto Marchisio, Muhammad Kashif, and Muhammad Shafique, "PO-QA: A Framework for Portfolio Optimization Using Quantum Algorithms," arXiv, July 29, 2024, https://arxiv.org/abs/2407.19857.

31. Mohammad Shamsuddoha, Mohammad Abul Kashem, Tasnuba Nasir, Ahamed Ismail Hossain, and Md Foysal Ahmed, "Quantum Computing Applications in Supply Chain Information and Optimization: Future Scenarios and Opportunities," *Information* 16, no. 8 (August 15, 2025): 693, https://doi.org/10.3390/info16080693; and Zhen-Song Chen, Yue Tan, Zheng Ma, Zhengze Zhu, and Mirosław J. Skibniewski, "Unlocking the Potential of Quantum Computing in Prefabricated Construction Supply Chains: Current Trends, Challenges, and Future Directions," *Information Fusion* 120 (2025): 103043, https://doi.org/10.1016/j.inffus.2025.103043.

32. Jirawat Tangpanitanon, "Quantum Computing for Energy Management: A Semi Non-Technical Guide for Practitioners," arXiv, November 15, 2024, https://arxiv.org/abs/2411.11901; Thomas Morstyn and Xiangyue Wang, "Opportunities for Quantum Computing Within Net-Zero Power System Optimization," *Joule* 8, no. 6 (2024): 1619–40, https://www.sciencedirect.com/science/article/pii/S2542435124001557; and Minghong Liu, Mengke Liao, Ruilong Zhang, Xin Yuan, Zhaoqun Zhu, and Zhi Wu, "Quantum Computing as a Catalyst for Microgrid Management: Enhancing Decentralized Energy Systems Through Innovative Computational Techniques," *Sustainability* 17, no. 8 (2025): 3662, https://www.mdpi.com/2071-1050/17/8/3662.

33. Stefano Olivares, “Quantum Computation with Trapped Ions,” in *A Student’s Guide to Quantum Computing* (Springer Nature Switzerland, 2025), 153–64, https://link-springer-com.ezproxy-prd.bodleian.ox.ac.uk/chapter/10.1007/978-3-031-83361-8_10.

34. Stefano Olivares, “Superconducting Qubits: Charge and Transmon Qubit,” in *A Student’s Guide to Quantum Computing*, 165–81.

35. Paul Steinacker, Nard Dumoulin Stuyck, Wee Han Lim, et al., “Industry-Compatible Silicon Spin-Qubit Unit Cells Exceeding 99% Fidelity,” *Nature*, September 24, 2025, https://doi.org/10.1038/s41586-025-09531-9.

36. Elham Hosseini Lapasar, Kenichi Kasamatsu, Yasushi Kondo, Mikio Nakahara, and Tetsuo Ohmi, “Implementation of a Selective Two-Qubit Gate Operation in a Neutral Atom Quantum Computer,” in *Quantum Information and Quantum Computing*, ed. Mikio Nakahara and Yoshitaka Sasaki (World Scientific, 2012), 43–49.

37. Stefano Olivares, “Two-Level Systems and Photonic Qubits,” in *A Student’s Guide to Quantum Computing*, 131–51.

38. Mikio Nakahara and Tetsuo Ohmi, “Quantum Gates, Quantum Circuit and Quantum Computation,” chap. 4 in *Quantum Computing: From Linear Algebra to Physical Realizations* (CRC Press, 2008), https://doi.org/10.1201/9781420012293.

39. Anthony Sudbery, “The Life and Entangled Adventures of Schrödinger’s Cat,” arXiv, August 8, 2023, https://arxiv.org/abs/2309.06387.

40. Vlatko Vedral, “Quantum Error Correction,” in *Introduction to Quantum Information Science*, chap. 13, 185, https://academic.oup.com/book/8602/chapter-abstract/154589645.

41. Google Quantum AI and collaborators, “Quantum Error Correction Below the Surface Code Threshold,” *Nature*, December 9, 2024, https://doi.org/10.1038/s41586-024-08449-y.

42. 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/.

43. The Quant, “The Price of a Quantum Computer,” *Quantum Zeitgeist*, May 1, 2024, https://quantumzeitgeist.com/the-price-of-a-quantum-computer-2/#google_vignette; and Karen Unland, “Zero Point Cryogenics Closes Deal Involving National Research Council,” *Taproot Edmonton*, September 23, 2022, https://edmonton.taproot.news/news/2022/09/23/zero-point-cryogenics-closes-deal-with-national-research-council.

44. Quantum Machines, Qblox, and Zurich Instruments are some of the firms developing modular control platforms with tighter integration. Intel is designing cryo-compatible chips that operate at cryogenic temperatures, potentially bringing classical processing directly into the quantum environment.

45. Google Quantum AI et al., “Quantum Error Correction.”

46. Sergey Bravyi, Andrew W. Cross, Jay M. Gambetta, Dmitri Maslov, Patrick Rall, and Theodore J. Yoder, “High-Threshold and Low-Overhead Fault-Tolerant Quantum Memory,” *Nature* 627, no. 8005 (March 27, 2024): 778–82, https://doi.org/10.1038/s41586-024-07107-7.

47. Laura Caune, Luka Skoric, Nick S. Blunt, et al., “Demonstrating Real-Time and Low-Latency Quantum Error Correction with Superconducting Qubits,” arXiv, October 7, 2024, https://arxiv.org/abs/2410.05202.

48. Companies such as Riverlane are developing custom hardware accelerators and algorithms to meet these demands.

49. Leon Riesebos, Brad Bondurant, Jacob Whitlow, et al., “Modular Software for Real-Time Quantum Control Systems,” *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, September 1, 2022, 545–55, https://doi.org/10.1109/qce53715.2022.00077; and Harrison Ball, Michael J. Biercuk, Andre R. R. Carvalho, et al., “Software Tools for Quantum Control: Improving Quantum Computer Performance Through Noise and Error Suppression,” *Quantum Science and Technology* 6, no. 4 (January 18, 2021): 044011, https://doi.org/10.1088/2058-9565/abdca6.

50. Examples include Qiskit (IBM), Cirq (Google), pyQuil (Rigetti), and PennyLane (Xanadu).

51. Jaime Sevilla and C. Jess Riedel, “Forecasting Timelines of Quantum Computing,” arXiv, September 10, 2020, https://arxiv.org/abs/2009.05045; “When Will a Quantum Computer Running Shor’s Algorithm (or a Similar One) Be Used to Factor One of the RSA Numbers for the First Time?,” Metaculus, opened February 20, 2020, https://www.metaculus.com/questions/3684/date-quantum-algorithm-factors-rsa-number/; Marin Ivezic, “Q-Day Revisited—RSA-2048 Broken by 2030: Detailed Analysis,” PostQuantum, June 19, 2025, https://postquantum.com/q-day/q-day-y2q-rsa-broken-2030/. Sevilla and Riedel (2020) predict quantum devices capable of factoring RSA-2048 are unlikely (<5% confidence) to exist before 2039, while Metaculus predicts this by 2033 and Ivezic (2025) predicts by 2030.

52. These products include Amazon Web Services (AWS) Braket, Azure Quantum, and IBM Quantum.

53. John Preskill, “Quantum Computing in the NISQ Era and Beyond,” *Quantum* 2 (August 6, 2018): 79, https://doi.org/10.22331/q-2018-08-06-79.

54. Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, et al., “Noisy Intermediate-Scale Quantum Algorithms,” *Reviews of Modern Physics* 94, no. 1 (February 15, 2022), https://doi.org/10.1103/revmodphys.94.015004; and Stefan Scheel, Barry Sanders, and Christoph Simon, “Optimising Algorithm Performance on NISQ Computers Using Machine Learning,” *Imaging Quantum Systems (IQS): Photons, Molecules, Materials*, 2021, https://www.iqs.uni-rostock.de/storages/uni-rostock/Alle_MNF/Physik_IRTG2676/Projects/IRTG_project_Scheel_NISQ.pdf.

55. Hanna Linn, Isak Lyngfelt, Laura García-Álvarez, and Göran Johansson, “Resource Analysis of Quantum Algorithms for Coarse-Grained Protein Folding Models,” *Physical Review Research* 6, no. 3 (July 26, 2024), https://doi.org/10.1103/physrevresearch.6.033112; and Pranav Chandarana, Narendra N. Hegade, Iraitz Montalban, Enrique Solano, and Xi Chen, “Digitized Counterdiabatic Quantum Algorithm for Protein Folding,” *Physical Review Applied* 20, no. 1 (July 12, 2023), https://doi.org/10.1103/physrevapplied.20.014024.

56. The Palo Alto–based PsiQuantum is an outlier, betting on fusion-based rather than gate-based architectures.

57. Vivien M. Kendon, Kae Nemoto, and William J. Munro, “Quantum Analogue Computing,” *Philosophical Transactions of the Royal Society A* 368, no. 1924 (July 5, 2010): 3609–20, https://doi.org/10.1098/rsta.2010.0017.

58. Atanu Rajak, Sei Suzuki, Amit Dutta, and Bikas K. Chakrabarti, “Quantum Annealing: An Overview,” *Philosophical Transactions of the Royal Society A* 381, no. 2241 (December 5, 2022), https://doi.org/10.1098/rsta.2021.0417.

59. D-Wave, for example, has offered annealing-based systems since 2011, yet these machines have not become broadly useful.

60. Chee Kong Lee, Pranay Patil, Shengyu Zhang, and Chang Yu Hsieh, “Neural-Network Variational Quantum Algorithm for Simulating Many-Body Dynamics,” *Physical Review Research* 3, no. 2 (May 5, 2021), https://doi.org/10.1103/physrevresearch.3.023095.

61. Jonathan Wei Zhong Lau, Kian Hwee Lim, Harshank Shrotriya, and Leong Chuan Kwek, “NISQ Computing: Where Are We and Where Do We Go?,” *AAPPS Bulletin* 32, no. 27 (September 26, 2022), https://doi.org/10.1007/s43673-022-00058-z.

62. Craig Gidney and Martin Ekerå, “How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits,” *Quantum* 5 (April 15, 2021): 433, https://doi.org/10.22331/q-2021-04-15-433.

63. Davide Castelvecchi, “IBM Releases First-Ever 1,000-Qubit Quantum Chip,” *Nature* 624, no. 7991 (December 4, 2023): 238, https://doi.org/10.1038/d41586-023-03854-1.

64. “Quantinuum Dominates the Quantum Landscape: New World-Record in Quantum Volume,” *Quantinuum Blog*, May 12, 2025, https://www.quantinuum.com/blog/quantum-volume-milestone; and “Debunking Algorithmic Qubits,” *Quantinuum Blog*, March 1, 2024, https://www.quantinuum.com/blog/debunking-algorithmic-qubits.

65. Gordon E. Moore, “Cramming More Components onto Integrated Circuits,” *Electronics*. 38, no. 8 (April 19, 1965), https://hasler.ece.gatech.edu/Published_papers/Technology_overview/gordon_moore_1965_article.pdf.

66. Michael Riordan and Lillian Hoddeson, *Crystal Fire: The Birth of the Information Age* (W. W. Norton, 1997).

67. Michael Bogobowicz, Kamalika Dutta, Martina Gschwendtner, et al., “Steady Progress in Approaching the Quantum Advantage,” McKinsey and Company Digital, April 24, 2024, https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/steady-progress-in-approaching-the-quantum-advantage#/.

68. “Quantum Computing on Track to Create up to $850 Billion of Economic Value by 2040,” Boston Consulting Group, July 18, 2024, https://www.bcg.com/press/18july2024-quantum-computing-create-up-to-850-billion-of-economic-value-2040.

69. Pricing varies by modality and architecture: Users pay per “shot” (a single execution of a quantum algorithm) or per “task” (a batch of shots). For now, QCaaS is used primarily in research, proof-of-concept experiments, and software development.

70. “Quantum Computer Cost in 2025: Surprisingly Cheap,” Quantum Zeitgeist, June 29, 2024, https://quantumzeitgeist.com/the-price-of-a-quantum-computer/.

71. John Levy, “1 Million Qubit Quantum Computers: Moving Beyond the Current ‘Brute Force’ Strategy,” *SEEQC* (blog), accessed October 5, 2025, https://seeqc.com/resources/1-million-qubit-quantum-computers-moving-beyond-the-current-%E2%80%9Cbrute-force%E2%80%9D-strategy.

72. Yuri Alexeev, Marwa H. Farag, Taylor L. Patti, et al., “Artificial Intelligence for Quantum Computing,” *Nature Communications* 16 (December 2, 2025): 10821, https://doi.org/10.1038/s41467-025-65836-3.

73. Laura Antoni-Micollier, Maxime Arnal, Romain Gautier, Camille Janvier, Vincent Ménoret, and Jeremie Richard, “Absolute Quantum Gravimeters and Gradiometers for Field Measurements,” *IEEE Instrumentation & Measurement Magazine* 27, no. 6 (September 2024): 4–10, https://ieeexplore.ieee.org/document/10654720.

74. Ben Stray, Andrew Lamb, Aisha Kaushik, et al., “Quantum Sensing for Gravity Cartography,” *Nature* 602 (2022): 590–94, https://www.nature.com/articles/s41586-021-04315-3.

75. Daniel Boddice, Nicole Metje, and George Tuckwell, “Capability Assessment and Challenges for Quantum Technology Gravity Sensors for Near Surface Terrestrial

Geophysical Surveying," *Journal of Applied Geophysics* 146 (November 2017): 149–59, https://doi.org/10.1016/j.jappgeo.2017.09.018.

76. Olivier Carraz, Luca Massotti, Aaron Strangfeld, Arnaud Heliere, Ilias Daras, and Pierluigi Silvestrin, "ESA Activities and Perspectives on Quantum Space Gravimetry," in *Proceedings of SPIE* 12777 (2023): 127773K, https://doi.org/10.1117/12.2690535.

77. Gage Taylor, "NASA Aims to Fly First Quantum Sensor for Gravity Measurements," NASA Science, April 15, 2025, https://science.nasa.gov/technology/technology-highlights/nasa-aims-to-fly-first-quantum-sensor-for-gravity-measurements/.

78. Xi Kong, Alexander Stark, Jiangfeng Du, Liam P. McGuinness, and Fedor Jelezko, "Towards Chemical Structure Resolution with Nanoscale Nuclear Magnetic Resonance Spectroscopy," *Physical Review Applied* 4 (2015): 024004, https://doi.org/10.1103/PhysRevApplied.4.024004.

79. "IndiPIX™: Paving the Way Towards Compact, Portable, and Cost-Effective Mid-wave Infrared Systems Imaging Systems," University of Glasgow, https://gla.portals.in-part.com/e9493bba-27fe-437e-be67-14b64d5dfcc3.

80. Holly Schofield, Ryan M. Hill, Odile Feys, et al., "A Novel, Robust, and Portable Platform for Magnetoencephalography Using Optically-Pumped Magnetometers," *Imaging Neuroscience* 2 (2024), https://doi.org/10.1162/imag_a_00283; and Nabeel Aslam, Hengyun Zhou, Elana K. Urbach, et al., "Quantum Sensors for Biomedical Applications," *Nature Reviews Physics* 5, no. 3 (2023): 157–69, https://doi.org/10.3390/s24030743.

81. "Qnami's Quantum Microscope – ProteusQ™," Qnami, accessed October 5, 2025, https://qnami.ch/portfolio/proteusq/.

82. Jens Pogorzelski, Ludwig Horsthemke, Jonas Homrighausen, Dennis Stiegekötter, Markus Gregor, and Peter Glösekötter, "Compact and Fully Integrated LED Quantum Sensor Based on NV Centers in Diamond," *Sensors* 24, no. 3 (2024): 743, https://doi.org/10.3390/s2403074.3.

83. "Bosch Establishes Company with the Synthetic Diamond Solutions Provider Element Six," Bosch Press Portal, April 7, 2025, https://www.bosch-presse.de/pressportal/de/en/bosch-establishes-company-with-the-synthetic-diamond-solutions-provider-element-six-274944.html.

84. Ronny Stolz, Markus Schiffler, Michael Becken, et al., "SQUIDs for Magnetic and Electromagnetic Methods in Mineral Exploration," *Mineral Economics* 35 (2022): 467–94, https://doi.org/10.1007/s13563-022-00333-3.

85. Yinan Hu, Geoffrey Z. Iwata, Mohaddese Mohammadi, et al., "Sensitive Magnetometry Reveals Inhomogeneities in Charge Storage and Weak Transient Internal Currents in Li-Ion Cells," *Proceedings of the National Academy of Sciences* 117, no. 20 (2020): 10667–72, https://pubmed.ncbi.nlm.nih.gov/32376633/.

86. Katarzyna Kubiak, "Quantum Technology and Submarine Near-Invulnerability," European Leadership Network, December 11, 2020, https://europeanleadershipnetwork.org/policy-brief/quantum-technology-and-submarine-near-invulnerability/.

87. Olga Sambataro, Riccardo Costanzi, Joao Alves, et al., "Current Trends and Advances in Quantum Navigation for Maritime Applications: A Comprehensive Review," *IEEE Journal of Oceanic Engineering* 50, no. 3 (April 15, 2025): 2101–34, https://ieeexplore.ieee.org/abstract/document/10965754.

88. Dana Goward, "Increasing GNSS Interference: UK and EU Warn Aviation," *GPS World*, April 11, 2023, https://www.gpsworld.com/increasing-gnss-interference-uk-and-eu-warn-aviation/.

89. Mia Jukić, Andrea Munafo, Pietro Paglierani, et al., "Quantum Sensing for Magnetic-Aided Navigation in GPS-Denied Environments," in *Proceedings of the SPIE Conference on Quantum Technologies for Defence and Security*, November 2024, https://doi.org/10.1117/12.3034019.

90. *National Quantum Initiative Supplement to the President's FY 2024 Budget*, Subcommittee on Quantum Information Science, Committee on Science, National Science & Technology Council, December 2023, https://www.quantum.gov/wp-content/uploads/2023/12/NQI-Annual-Report-FY2024.pdf.

91. H. Vella, "Quantum Radars Expose Stealth Planes," *Engineering & Technology* 14, no. 4 (May 2019): 42–45, https://doi.org/10.1049/et.2019.0402; and Shabir Barzanjeh, Saikat Guha, Christian Weedbrook, David Vitali, Jeffrey H. Shapiro, and Stefano Pirandola, "Microwave Quantum Illumination," *Physical Review Letters* 114, no. 8 (2015): 080503, https://doi.org/10.1103/PhysRevLett.114.080503.

92. Athena Karsa, Alasdair Fletcher, Gaetana Spedalieri, and Stefano Pirandola, "Quantum Illumination and Quantum Radar: A Brief Overview," *Reports on Progress in Physics* 87, no. 9 (2024): 094001, https://doi.org/10.1088/1361-6633/ad6279; and Jeffrey H. Shapiro, "The Quantum Illumination Story," *IEEE Aerospace and Electronic Systems Magazine* 35, no. 4 (April 1, 2020): 8–20, https://ieeexplore.ieee.org/abstract/document/9087936.

93. A. E. E. Dubois, D. A. Broadway, A. Stark, et al., "Untrained Physically Informed Neural Network for Image Reconstruction of Magnetic Field Sources," *Physical Review Applied* 18 (2022): 064076, https://doi.org/10.1103/PhysRevApplied.18.064076; Valeria Cimini, Mauro Valeri, Emanuele Polino, et al., "Deep Reinforcement Learning for Quantum Multiparameter Estimation," *Advanced*

Photonics 5, (2023): 016005, https://doi.org/10.1117/1.AP.5.1.016005; and Tailong Xiao, Jianping Fan, and Guihua Zeng, "Parameter Estimation in Quantum Sensing Based on Deep Reinforcement Learning," *npj Quantum Information* 8, (2022): 2, https://doi.org/10.1038/s41534-021-00513-z.

94. Heather Landi, "Mayo Clinic Taps Startup SandboxAQ to Study New Tech—Quantum Sensing and AI—for Cardiac Diagnostics," Fierce Healthcare, August 8, 2024, https://www.fiercehealthcare.com/ai-and-machine-learning/mayo-clinic-taps-startup-sandboxaq-study-new-tech-quantum-sensing-and-ai.

95. Fernando Dominguez Pinuaga, Andrea Bortolato, Alfonso Muñoz Muñoz, and Stefan Bogdanovic, "Practical Realities: How AI Empowers Quantum Technologies to Solve Today's Biggest Challenges," *SandboxAQ* (blog), April 30, 2024, https://www.sandboxaq.com/post/practical-realities-how-ai-empowers-quantum-technologies-to-solve-todays-biggest-challenges.

96. Moeta Tsukamoto, Shuji Ito, Kensuke Ogawa, Yuto Ashida, Kento Sasaki, and Kensuke Kobayashi, "Accurate Magnetic Field Imaging Using Nanodiamond Quantum Sensors Enhanced by Machine Learning," *Scientific Reports* 12 (2022): 13942, https://doi.org/10.1038/s41598-022-18115-w.

97. Gidney, "How to Factor 2048 Bit RSA Integers with Less Than a Million Noisy Qubits."

98. Madelyn Cain, Qian Xu, Robbie King, et al., "Shor's Algorithm Is Possible with as Few as 10,000 Reconfigurable Atomic Qubits," arXiv, March 30, 2026, https://doi.org/10.48550/arXiv.2603.28627.

99. Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, "The Security of Practical Quantum Key Distribution," *Reviews of Modern Physics* 81, no. 3 (2009): 1301, https://doi.org/10.1103/RevModPhys.81.1301.

100. Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov, "Full-Field Implementation of a Perfect Eavesdropper on a Quantum Cryptography System," *Nature Communications* 2 (2011): 349, https://doi.org/10.1038/ncomms1348.

101. Chris Jay Hoofnagle and Simson L. Garfinkel, *Law and Policy for the Quantum Age* (Cambridge University Press, 2022), https://doi.org/10.1017/9781108883719.

102. Aitor Brazaola-Vicario, Alejandra Ruiz, Oscar Lage, Eduardo Jacob, and Jasone Astorga, "Quantum Key Distribution: A Survey on Current Vulnerability Trends and Potential Implementation Risks," *Optics Continuum* 3 (2024): 1438–60, https://doi.org/10.1364/OPTCON.530352.

103. Umang Dubey, Prathamesh Bhole, Arindam Dutta, et al., "A Review on Practical Challenges of Aerial Quantum Communication," *Physics Open* 19 (May 2024): 100210, https://doi.org/10.1016/j.physo.2024.100210; and Hong-fu Chou, Vu Nguyen Ha, Hayder Al-Hraishawi, et al., "Satellite-Based Quantum Network: Security and Challenges over Atmospheric Channel," arXiv, September 17, 2023, https://doi.org/10.48550/arXiv.2308.00011.

104. Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, et al., "Satellite-Relayed Intercontinental Quantum Network," *Physical Review Letters* 120, no. 3 (2018): 030501, https://doi.org/10.1103/PhysRevLett.120.030501.

105. Yang Liu, Wei-Jun Zhang, Cong Jiang, et al., "Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance," *Physical Review Letters* 130, no. 21 (May 26, 2023): 210801, https://doi.org/10.1103/PhysRevLett.130.210801.

106. Naphan Benchasattabuse, Michal Hajdušek, and Rodney Van Meter, "Engineering Challenges in All-Photonic Quantum Repeaters," arXiv, May 16, 2024, https://doi.org/10.48550/arXiv.2405.09876.

107. Hoofnagle and Garfinkel, *Law and Policy*, 258.

108. "Post-Quantum Cryptography," NIST Computer Security Resource Center, accessed October 5, 2025, https://csrc.nist.gov/projects/post-quantum-cryptography.

109. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," The White House, May 4, 2022, https://bidenwhitehouse.archives.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/.

110. *Report on Post-Quantum Cryptography* (The White House, 2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf.

111. "IBM Announces Quantum Milestone," Bloomberg Technology, June 20, 2025, YouTube video, 6:09, https://www.youtube.com/watch?v=FCeuVND6fuY&t=80s.

112. "National Security Memorandum."

113. National Quantum Initiative Act, H.R. 6227, 115th Cong. (2018), Congress.gov, accessed October 5, 2025, https://www.congress.gov/bill/115th-congress/house-bill/6227/text. The primary agencies included in NQI are NIST, NSF, and DOE. While they receive funding for quantum activities, NASA and DoD are only mentioned once in the NQI text as members of the subcommittee on quantum information science.

114. "National Security Memorandum."

115. Defense Science Board, *Applications of Quantum Technologies* (US Department of Defense, 2019),

https://apps.dtic.mil/sti/trecms/pdf/AD1090337.pdf; and "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," NSA/CSS, accessed October 5, 2025, https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

116. "Virtual Event: Advancing America's Quantum Leadership with Next-Generation Sensors," Center for a New American Security, August 27, 2025, https://www.cnas.org/events/virtual-event-advancing-americas-quantum-leadership-with-next-generation-sensors.

117. "习近平在中央政治局第二十四次集体学习时强调深刻认识 . . ." ["Xi Jinping emphasizes the profound understanding of . . . during the 24th Collective Study Session of the Politburo"], 新华网 [Xinhua News Agency], October 17, 2020, https://www.xinhuanet.com/politics/2020-10/17/c_1126623288.htm; and "瞭望· 瞭望访谈 | 加速量子计算落地——专访中国科学院院士郭光灿" ["Outlook Interview | Accelerating the realization of quantum computing—interview with CAS academician Guo Guangcan"], 腾讯新闻 [Tencent News], August 26, 2024, https://news.qq.com/rain/a/20240826A09OMI00.

118. 崔爽 [Cui Shuang], "全球首例！我国量子密码技术实现双重加密里程碑" ["A world first! China achieves a milestone in dual encryption using quantum cryptography technology"], 科技日报 [Science and Technology Daily], May 14, 2025, https://www.stdaily.com/web/gdxw/2025-05/14/content_339296.html.

119. "Alibaba Shuts Quantum Computing Lab in Sign of Broader Cutback," Bloomberg, November 26, 2023, https://www.bloomberg.com/news/articles/2023-11-27/alibaba-shuts-quantum-computing-lab-in-sign-of-broader-cutback; and "Baidu to Donate Quantum Computing Lab, Equipment to Beijing Institute," Reuters, January 3, 2024, https://www.reuters.com/technology/baidu-donate-quantum-computing-lab-equipment-beijing-institute-2024-01-03/.

120. Hao-Ze Chen, Ming-Han Li, Yu Zhou Wang, et al., "Implementation of Carrier-Grade Quantum Communication Networks over 10,000 km," *npj Quantum Information* 11 (2025): 137, https://doi.org/10.1038/s41534-025-01089-8.

121. Zhang Tong, "Chinese Firm Launches 'Unhackable' Quantum Cryptography System," *South China Morning Post*, May 18, 2025, https://www.scmp.com/news/china/science/article/3310817/chinese-firm-launches-unhackable-quantum-cryptography-system.

122. "ICBC Succeeds in Applying Thousand-km-Level Quantum Communication Technology," ICBC, May 2, 2017, https://www.icbc-ltd.com/icbc/en/newsupdates/icbc%20news/ICBCSucceedsinApplyingThousandkmlevelQuantumCommunicationTechnology.htm.

123. 崔爽 [Cui Shuang], "全球首个双重加密量子密码体系发布" ["The world's first dual-encryption quantum cryptography system released"]," 科技日报 [Science and Technology Daily], May 19, 2025, https://www.stdaily.com/web/gdxw/2025-05/19/content_341657.html.

124. "中国量子科技加快实现天地一体化" ["China accelerates the integration of quantum science and technology across Earth and space"], 国务院 [The State Council of the People's Republic of China], November 10, 2020, https://www.gov.cn/xinwen/2020-11/10/content_5560121.htm.

125. Dongxin Gao, Daojin Fan, Chen Zha, et al., "Establishing a New Benchmark in Quantum Computational Advantage with 105-Qubit Zuchongzhi 3.0 Processor," *Physical Review Letters* 134, no. 9 (March 3, 2025): 090601, https://doi.org/10.1103/PhysRevLett.134.090601; Qingling Zhu, Sirui Cao, Fusheng Chen, et al., "Quantum Computational Advantage via 60-Qubit 24-Cycle Random Circuit Sampling," *Science Bulletin* 67, no. 3 (February 15, 2022): 240–45, https://doi.org/10.1016/j.scib.2021.10.017; and "瞭望 | 中国量子科技，只看这一篇就够了" ["Outlook | China's quantum technology: This one article says it all"], 清华大学新闻网 [Tsinghua University News Network], December 22, 2021, https://www.tsinghua.edu.cn/info/1182/90238.htm.

126. "Quantinuum Dominates the Quantum Landscape"; M. C. Smith, A. D. Leu, K. Miyanishi, M. F. Gely, and D. M. Lucas, "Single-Qubit Gates with Errors at the 10^{-7} Level," arXiv, December 5, 2024, https://doi.org/10.48550/arXiv.2412.04421; and Hartmut Neven, "Meet Willow, Our State-of-the-Art Quantum Chip," Google, December 9, 2024, https://blog.google/technology/research/google-willow-quantum-chip/.

127. Brian Hart, Bonny Lin, Samantha Lu, Hannah Price, Yu-jie (Grace) Liao, and Matthew Slade, "Is China a Leader in Quantum Technologies?," ChinaPower, August 14, 2023, updated January 31, 2024, https://chinapower.csis.org/china-quantum-technology/; and Elliott Mason, "Quantum Patent Trends Update: 2022," QED-C, February 13, 2023, https://quantumconsortium.org/publication/quantum-patent-trends-update-2022/.

128. "阿里确认放弃量子计算研发，实验室裁撤，设备送浙大" ["Alibaba confirms it has abandoned quantum computing research; laboratory disbanded, equipment sent to Zhejiang University"], 澎湃新闻 [The Paper], November 28, 2023, https://www.thepaper.cn/newsDetail_forward_25443390; and "百度和阿里巴巴退出量子電腦研發 聚焦人工智慧應用" ["Baidu and Alibaba withdraw from quantum computer research to focus on artificial intelligence applications"], Tech Nice, January 18, 2024, https://www.technice.com.tw/technology/software/92237/.

129. "中国量子科技加快实现天地一体化" ["China accelerates the integration"].

130. "China Successfully Develops Quantum Radar System," *People's Daily Online*, September 8, 2016, https://en.people.cn/n3/2016/0908/c98649-9112553.html.

131. Dannie Peng, "'Two Sessions' 2024: Chinese Lawmaker Urges Beijing to Safeguard Tech Production Chain to Give Nation a Quantum Edge," *South China Morning Post*, March 1, 2024, https://www.scmp.com/news/china/science/article/3253846/two-sessions-2024-chinese-lawmaker-urges-beijing-safeguard-tech-production-chain-give-nation-quantum.

132. Edward Parker, Daniel Gonzales, Ajay K. Kochhar, et al., "An Assessment of the US and Chinese Industrial Bases in Quantum Technology," RAND Corporation, February 2, 2022, https://www.rand.org/pubs/research_reports/RRA869-1.html.

133. Areas where Europe leads include neutral atoms, control stacks, and cryo-CMOS systems.

134. "2025 Research Leaders: Leading Countries/Territories," Nature Index, accessed October 6, 2025, https://www.nature.com/nature-index/research-leaders/2025/country/all/global.

135. "中国科技出版物数量首次超过美国" ["For the first time, the number of China's scientific publications exceeds that of the US"], 国家自然科学基金委员会 [National Natural Science Foundation of China], accessed October 6, 2025, https://www.nsfc.gov.cn/csc_phone/kqkd29/kjyq1/20715/index.html.

136. After some embarrassing revelations, China officially banned financial rewards in 2020, but it likely still offers professional incentives to scientists to publish more. See Ren Mengshan, "过于追求 ESI 排名是学术功利主义" ["Over-pursuing ESI rankings is academic utilitarianism"], 光明网 [Guangming Daily], December 3, 2019, https://news.gmw.cn/2019-12/03/content_33368526.htm; and Smriti Mallapaty, "China Bans Cash Rewards for Publishing Papers," *Nature* 579 (2020): 18, https://doi.org/10.1038/d41586-020-00574-8.

137. Wei Quan, Bikun Chen, and Fei Shu, "Publish or Impoverish: An Investigation of the Monetary Reward System of Science in China (1999–2016)," *Aslib Journal of Information Management* 69, no. 5 (September 18, 2017): 486–502, https://doi.org/10.1108/AJIM-01-2017-0014; and Shumin Qiu, Claudia Steinwender, and Pierre Azoulay, "Paper Tiger? Chinese Science and Home Bias in Citations," NBER Working Paper No. 32468, May 2024, https://www.nber.org/system/files/working_papers/w32468/w32468.pdf.

138. Richard Van Noorden, "Exclusive: These Universities Have the Most Retracted Scientific Articles," *Nature* 638 (2025): 596–99, https://doi.org/10.1038/d41586-025-00455-y.

139. Henning Soller, Martina Gschwendtner, Sara Shabani, and Waldemar Svejstrup, *The Year of Quantum: From Concept to Reality in 2025* (*Quantum Technology Monitor* report, McKinsey & Company, 2025), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025#/.

140. Elliott J. Mason, "State of Quantum Industry Innovation—What Patents Tell Us," QED-C, December 11, 2024, https://quantumconsortium.org/publication/state-of-quantum-industry-innovation-what-patents-tell-us/.

141. Parker et al., "An Assessment of the US and Chinese Industrial Bases."

142. Mason, "State of Quantum Industry Innovation."

143. "中国量子科技加快实现天地一体化," [China accelerates the integration].

144. "China to Set Up National Venture Capital Guidance Fund, State Planner Says," Reuters, March 6, 2025, https://www.reuters.com/world/china/china-set-up-national-venture-capital-guidance-fund-state-planner-says-2025-03-06/; and Cui Lei, "Chinese Quantum Computing Startup Origin Quantum Closes $148M in Series B Round," CAS Fund of Funds (China Science and Technology Innovation Fund), July 22, 2022, http://en.casfof.com/news/22.html.

145. "From Lab to Industry, Hefei Accelerates Quantum Leap," Science and Technology Daily (via Standard Daily), July 19, 2025, https://www.stdaily.com/web/English/2025-07/11/content_368407.html.

146. Olivier Ezratty, *Understanding Quantum Technologies 2024* (independently published, 2024), accessed October 6, 2025, https://www.oezratty.net/wordpress/2024/understanding-quantum-technologies-2024/.

147. "Addressing the US Quantum Labor Shortage Before It's Too Late," MeriTalk, accessed October 6, 2025, https://www.meritalk.com/addressing-the-u-s-quantum-labor-shortage-before-its-too-late/; and National Center for Science and Engineering Statistics, "Nearly Half of 2023 US Doctorate Recipients with Temporary Visas Were from China or India," NSF report 25-336 (National Science Foundation, 2025), https://ncses.nsf.gov/pubs/nsf25336.

148. Parker et al., "An Assessment of the US and Chinese Industrial Bases"; Jane Cai, "Does a Talent Crisis Threaten China's Quantum Ambitions? One Chinese Expert Thinks So," *South China Morning Post*, October 24, 2024, https://www.scmp.com/news/china/politics/article/3283730/involution-biggest-threat-chinas-quantum-computing-field-internal-risk-expert; and Jeroen Groenewegen-Lau and Antonia Hmaidi, *Where China Stands in the Global Race for Talent* (MERICS, 2024), https://merics.org/sites/default/files/2024-04/WP%20-%20Where%20china%20stands%20in%20the%20global%20race%20for%20talent%20-%20MERICS%20-%20final.pdf.

149. "全国人大代表郭国平：以中国自主体系加速培育量子人才" ["NPC Deputy Guo Guoping: Accelerating the cultivation of

quantum talent through China’s independent system”], 经济参考报 [Economic Information Daily], March 10, 2025, https://finance.sina.com.cn/tech/roll/2025-03-10/doc-inepcncs0898501.shtml; and “中国科学院院士郭光灿：量子计算人才紧缺，本土培养是关键” [“Guo Guangcan, academician of the Chinese Academy of Sciences: Quantum computing talent is scarce, local training is key”], 中国科学技术大学新闻网 [University of Science and Technology of China News Network], January 25, 2024, https://news.ustc.edu.cn/info/1056/87115.htm.

150. “MOE Press Conference Presents China’s Educational Achievements in 2023,” Ministry of Education of the People’s Republic of China, March 3, 2024, http://en.moe.gov.cn/news/press_releases/202403/t20240311_1119782.html; “Shenzhen Gezhi Academy: Establishing a Quantum Computing Demonstration School, Exploring a New Talent Cultivation Model,” SPINQ, June 6, 2023, https://www.spinquanta.com/news-detail/shenzhen-gezhi-academy-establishing-a-quantum-computing-demonstration-school-exploring20250121080944; and Holly Chik, “How Mainland China Streamlines National Labs into Tech War Machines: The Hong Kong Case,” *South China Morning Post*, August 30, 2025, https://www.scmp.com/news/china/science/article/3323633/how-china-streamlines-national-labs-tech-war-machines-case-study-hk.

151. *Strategic Research and Industry Agenda* (Quantum Flagship, 2024), https://qt.eu/media/pdf/Strategic-Reseach-and-Industry-Agenda-2030.pdf.

152. “Virtual Event: Advancing America’s Quantum Leadership with Next-Generation Sensors,” Center for a New American Security (CNAS), August 27, 2025, https://www.cnas.org/events/virtual-event-advancing-americas-quantum-leadership-with-next-generation-sensors.

153. Alan Geller, “Introducing Quantum Intermediate Representation (QIR),” Microsoft Quantum, accessed October 6, 2025, https://quantum.microsoft.com/en-us/insights/blogs/qir/introducing-quantum-intermediate-representation-qir.

154. Parker et al., “An Assessment of the US and Chinese Industrial Bases.”

155. “Commerce Lists Entities Involved in the Support of PRC Military Quantum Computing Applications, Pakistani Nuclear and Missile Proliferation, and Russia’s Military,” Bureau of Industry and Security, US Department of Commerce, November 24, 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-lists-entities-involved-support-prc-military-quantum-computing.

156. “Fact Sheet: Delivering on the Next Generation of Innovation and Partnership with Australia,” The White House, October 25, 2023, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/10/25/fact-sheet-delivering-on-the-next-generation-of-innovation-and-partnership-with-australia/; and “$2.7 Million for Cutting-Edge Quantum Optical Atomic Clocks,” Australian Department of Defence, September 13, 2024, https://www.defence.gov.au/news-events/releases/2024-09-13/27-million-cutting-edge-quantum-optical-atomic-clocks.

157. “International Traffic in Arms Regulations: Exemption for Defense Trade and Cooperation Among Australia, the United Kingdom, and the United States,” 89 Fed. Reg. 51,213 (August 20, 2024), https://www.federalregister.gov/documents/2024/08/20/2024-18043/international-traffic-in-arms-regulations-exemption-for-defense-trade-and-cooperation-among.

31 30 29 28 27 26 7 6 5 4 3 2 1

Preferred citation: Eyck Freymann, Sebastian Orbell, Sophie Coste, and Katharina Klotz, *The Quantum Revolution: A Guide for Allied Policymakers*, Allied Coordination and Applied History Working Groups, Hoover Institution, July 2026.

Cover image: iStock.com/Peter Hansen

ABOUT THE AUTHORS

EYCK FREYMANN

Eyck Freymann is a Hoover Fellow at Stanford University, where he directs the Allied Coordination Working Group and participates in the Applied History Working Group. He is the author of several books, including *Defending Taiwan*, *The Arsenal of Democracy*, and *One Belt One Road*.

SOPHIE COSTE

Sophie Coste is an analyst at Greenmantle, a geopolitical advisory firm, where she researches emerging tech, US-China competition, and economic choke points. She worked previously on energy security at the Center for Strategic and International Studies and at SAFE's critical minerals center. She holds a BS from the School of Foreign Service at Georgetown University.

SEBASTIAN ORBELL

Sebastian Orbell is a physicist and engineer on the Quantum Control team at Quantum Machines, where he builds agentic AI systems for the autonomous operation of spin and superconducting quantum computers. He holds a DPhil from the University of Oxford, specializing in physics-aware AI agents and high-fidelity qubit calibration.

KATHARINA KLOTZ

Katharina Klotz is a DPhil candidate at the University of Oxford, researching the impact of dual-use technology on states' economic and military security strategies. She is also the Europe analyst at Greenmantle. Previously, she researched the geopolitics of space and quantum technologies at the Oxford Internet Institute and the Oxford China Policy Lab.

SYNOPSIS

Quantum technologies are moving from the laboratory toward strategic relevance but at different speeds and with different implications for allied security. This report offers nontechnical policymakers in allied countries a comprehensive guide to quantum computing, sensing, and communications: where each stands, how China is competing, and why no single nation can control the stack. It argues that US leadership in the quantum era will depend on orchestrating resilient alliance networks.

Allied Coordination Working Group

The Hoover Institution's Allied Coordination Working Group (ACWG) designs actionable, integrated strategies to help allied democracies compete more effectively with China. It is housed within the Hoover History Lab, which uses history to address contemporary policy challenges. The ACWG works closely with several other Hoover groups and draws on the expertise of colleagues at the Centre for Geopolitics at the University of Cambridge and the Institute of Geoeconomics in Tokyo. It provides impetus for allied experts and policymakers to consult about their interests, needs, and capabilities—and to develop strategies collaboratively, from first principles to operational design.

Applied History Working Group

The Hoover Applied History Working Group aims to conduct and disseminate historical research on issues of national and international concern; provide concrete recommendations on the basis of research and discussion; and use Hoover's unique situation to convene academic experts, policymakers, and interested private-sector actors both at Stanford and in Washington, DC.

For more information about these Hoover Institution working groups, visit us online at hoover.org/research-teams/allied-coordination-working-group and hoover.org/research-teams/applied-history-working-group.

Hoover Institution
Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution
in Washington
1399 New York Ave. NW, Ste. 500
Washington, DC 20005
202-760-3200

Hoover Institution
in Texas
3889 Maple Ave., Ste. 600
Dallas, TX 75219
hoovertexas@stanford.edu

HOOVER INSTITUTION