FOREIGN AFFAIRS

JANUARY/FEBRUARY 2025• VOLUME 104 • NUMBER 1

The Race to Lead the Quantum Future

How the Next Computing Revolution Will Transform the Global Economy and Upend National Security

CHARINA CHOU, JAMES MANYIKA, AND HARTMUT NEVEN

The Race to Lead the Quantum Future

How the Next Computing Revolution Will Transform the Global Economy and Upend National Security

CHARINA CHOU, JAMES MANYIKA, AND HARTMUT NEVEN

Over the last several years, as rapid advances in artificial intelligence have gained enormous public attention and critical scrutiny, another crucial technology has been evolving largely out of public view. Once confined to the province of abstract theory, quantum computing seeks to use operations based on quantum mechanics to crack computational problems that were previously considered unsolvable. Although the technology is still in its infancy, it is already clear that quantum computing could have profound implications for national security and the global economy in the decades to come.

Since the late 2010s, the United States and many other advanced countries have become increasingly involved in the race for leadership

CHARINA CHOU is Director and Chief Operating Officer at Google Quantum AI.

JAMES MANYIKA is Senior Vice President at Google and its President for Research, Technology, and Society.

HARTMUT NEVEN is Vice President of Engineering at Google and Head of Google Quantum AI.

Illustration by Keith Negley

in quantum information science and technology, a field that encompasses quantum computing, quantum communications, and quantum sensing. Over the last decade, governments in 20 countries have announced investments in quantum development totaling more than $40 billion worldwide; China alone has committed to spend $15.3 billion over five years. In 2016, Beijing designated the development of quantum technologies as a national priority, and it has created advanced hubs for production. For its part, the United States, in 2018, enacted the National Quantum Initiative, legislation aimed at maintaining the country's technological and scientific lead in quantum information and its applications. The U.S. government has announced $3.7 billion in unclassified funding, plus more funding for defense research and development. In addition to government-led initiatives, multiple research and development efforts are underway in the private sector and academia.

Quantum machines could unlock breakthroughs rivaling those now projected to come from AI.

Although these investments are still dwarfed by U.S. and international funding for AI, the rise of quantum technology has already begun to shape international policy. In 2019, the United States announced a bilateral "statement on quantum cooperation" with Japan, which the U.S. government strengthened in 2023. And in 2024, Washington established a multilateral initiative called the Quantum Development Group to coordinate strategies for advancing and managing the new technology. The United States has also discussed quantum issues within various economic and security forums, including AUKUS, the trilateral defense pact among Australia, the United Kingdom, and the United States; the Quad, or Quadrilateral Security Dialogue, among Australia, India, Japan, and the United States; and the U.S.-EU Trade and Technology Council. Underscoring the growing concerns about the technology in Washington, one analyst for the Center for a New American Security argued in November, following the U.S. presidential election, that the incoming administration must "act quickly during the first 100 days to reinvigorate America's quantum competitiveness."

Thus far, the advent of quantum technology has been perceived largely as a national security issue. Since the 1990s, researchers have

recognized that one of the greatest threats posed by a powerful quantum computer is its potential as a code-breaking tool, capable of penetrating the encryption used by the most advanced communication systems and digital networks around the world today. This concern has spurred the U.S. government to develop and advocate for the adoption of quantum-resistant cryptography, strengthen export controls on quantum technology and related products, and build action-oriented partnerships with industry, academia, and local governments.

But the focus on code breaking has led policymakers to ignore other important applications of quantum technology. In fact, before quantum machines are able to crack advanced encryption systems—a capability that will require enormous computational power even after the technology is developed—they could have a transformational effect in many sectors of the economy, including energy and pharmaceuticals. Effectively harnessed, quantum technologies could spur innovation, scientific discovery, economic growth, and opportunity. In sheer human impact, some of the breakthroughs that could be unlocked by quantum machines rival those that are now projected to come from AI. For this reason, it is especially important that the technology is developed in open societies, with clear guardrails in place to ensure that it is used for benevolent purposes.

Winning the quantum race will not be easy. China has already taken the lead in some areas such as quantum communications, and in the coming years, focused American innovation and leadership will be critical to maintain U.S. competitiveness. The United States and its international partners will need to commit far more resources to bring their quantum projects to fruition, and they will have to develop quantum industries and a strong quantum supply chain to support these projects. If the United States and its allies fail to make these efforts a central strategic goal and policymaking priority, they could lose diplomatic influence, military might, and the ability to provide oversight of a powerful new technology. They could also miss out on the chance to forge a new path for economic and societal progress.

EVERYWHERE ALL AT ONCE

The concept of a quantum computer was first proposed by the theoretical physicist and Nobel laureate Richard Feynman in 1981.

Feynman came of age during the dawn of quantum mechanics, when scientists began to recognize that atoms, electrons, light, and other sub-nanoscale objects—building blocks for everything in the universe—obey fundamentally different rules than the objects of everyday life. Unlike, for example, a ball, which follows the straightforward rules of classical mechanics, electrons behave simultaneously as particles and waves, and their location cannot be exactly defined.

Feynman's insight was that to truly understand the quantum mechanical world—and the general workings of the universe itself—it would be necessary to build a computer that operates according to the same laws. "Nature isn't classical, dammit," he said, "and if you want to make a simulation of nature, you'd better make it quantum mechanical." Feynman's insight has turned out to be prescient. In the more than four decades since, computers following the "classical" design have utterly transformed the planet: pocket-sized mobile phones today are a million times as powerful as the hulking desktop personal computers of the 1980s. Moore's law—the prediction that the number of transistors on a computer chip would double every two years—has continued to broadly hold true in the semiconductor industry, despite multiple predictions of its demise. And the best supercomputers today can handle a quintillion—that is, a billion billion—operations per second. Yet as this revolution continues to mature, it has become increasingly clear that some computations are and will remain beyond even the best classical computers.

This is because existing computer technologies are constrained by the basic premise on which they operate. All forms of classical computing, whether an abacus, a personal laptop, or a high-performance cluster of machines in a national security facility, follow what scholars call Boolean logic. In this system, the basic unit of information is a bit, which is an object that can assume one of two states, conventionally referred to as 0 or 1. Although this system has proved highly efficient for many kinds of calculations, it cannot perform those of exceeding complexity, such as factoring a thousand-digit number, calculating the reaction dynamics of a molecule with hundreds of atoms, or solving certain kinds of optimization problems that are common in many fields.

In contrast, by harnessing quantum mechanics, quantum computing does not have the same constraints. A lesson of quantum physics—one that is startling and counterintuitive—is that particles can

exist in a simultaneous combination of multiple states. Accordingly, instead of bits, with their either-or operation, quantum computing uses a quantum bit, or qubit, which is a system that can be simultaneously in states 0 and 1. This both-at-once ability, known as superposition, conveys an enormous computational advantage, one that increases when more qubits are working together. Whereas a classical computer must process one state after another sequentially, a quantum computer can explore many possibilities in parallel. Think of trying to find the correct path through a maze: a classical computer has to try each path one by one; a quantum computer can explore multiple paths simultaneously, making it orders of magnitude faster for certain tasks. It is important to note that contrary to popular simplification, a quantum computer is not simply an enormous set of classical computers working in parallel. Although there are exponentially many possible answers that can be explored through a quantum processor, only one combination can be measured in the end. Deriving a solution from a quantum computer thus requires clever programming that amplifies the correct answer.

A major challenge is figuring out how to build quantum processors that are large and stable enough to produce consistent results for meaningful problems. Such processors tend to be extremely sensitive to their environment and can be easily affected by changes in temperature, vibrations, and other disturbances, which can lead to a variety of errors in the system. Since computational fidelity relies on qubits maintaining coherence, researchers are investing heavily in methods to improve qubit quality, including new designs, chip-fabrication processes, and techniques to correct for qubit error.

Currently, there is a wide array of approaches to designing qubits, each with its own advantages and drawbacks. In principle, any quantum mechanical system—atoms, molecules, ions, photons—could be fashioned into a qubit. In practice, factors such as manufacturability, controllability, performance, and computational speed dictate the most viable paths. Today's leading efforts include superconducting, neutral atom, photonic, and ion trap qubits. It is unclear at this early stage which, if any, will turn out to be successful. Beyond building the processor, other challenges include how to package the qubits, transmit their signals, and run applications. Researchers must use cryogenic refrigerators, which can cool superconducting qubits to within thousandths of a degree above absolute

zero, to provide an ultracold, dark, and quiet environment for operation. Expertise across these highly specialized components comes from disparate sources in many countries. Today, there are various "full-stack" quantum computing companies, including Amazon, Google, IBM, and QuEra, that are trying to integrate components into a final product. In short, quantum computing today faces a multitude of challenges and unknowns, and continued development will require a host of engineering innovations. What is clear is that for any of the approaches to succeed, they must be reliable, scalable, and cost effective.

THE NEW ANSWERING MACHINES

The race to arrive at a full-scale quantum computer is driven by several motives. Most fundamentally, quantum computing promises to provide answers to problems previously thought unsolvable—puzzles that would take eons for the world's best classical computers to crack. The most well-known problem of this kind is integer factorization, or breaking down a number as a product of several smaller numbers: even the fastest supercomputers are unable to factor very large numbers. This has meant that the most advanced forms of cryptography—which are based on factorization—cannot now be broken. But quantum computers may change that.

In 1994, the computer scientist Peter Shor proved that a quantum computer would be able to factor very large numbers. At the time, such a computer remained firmly in the realm of theory, but as the technology has begun to develop, Shor's insight has led to concerns that quantum processors may one day be capable of breaking even the most advanced encryption. Today, national security experts assume that hostile state and private actors are already collecting encrypted information in anticipation of the new technology, an approach known as a "store now, decrypt later" attack.

But decryption is only one possible application for quantum computers, and it is likely more than a decade away. As Feynman intuited, more obvious uses for quantum-based computing relate to quantum simulation—the ability to make exact calculations of quantum systems such as electrons, molecules, and materials—and these applications could begin to come into use sooner. Quantum processors are already contributing to discoveries in a number of highly specialized areas in physics—including quasiparticle engineering, many-body

dynamics, spin transport, metallic transport, time crystals, wormhole dynamics, and magnetization. With a full-scale, full-capability quantum computer, the possibilities are astounding. Consider agricultural fertilizers. At present, nitrogen fixation—the chemical process required to produce ammonia from nitrogen gas—is hugely energy intensive, accounting for as much as two percent of the world's annual energy budget. This is because the industrial catalysts used in this reaction are highly inefficient. In fact, the naturally occurring FeMoco molecule, a catalyst for biological nitrogen fixation, is far more efficient, but it cannot yet be chemically synthesized or isolated in industrial-scale quantities, and its mechanism of action has proven too challenging for existing computing technology to elucidate. With quantum computers, however, researchers may be able to perform the difficult calculations necessary to learn FeMoco's reaction mechanism, allowing the design of FeMoco-inspired catalysts that could save vast amounts of energy.

Winning the quantum race will not be easy.

Or take pharmaceuticals, which require drug molecules to interact effectively with molecules inside the body. To simulate the behavior of cytochrome P450, a family of enzymes largely responsible for drug metabolism and therefore how patients will respond to drugs, classical computers would require colossal amounts of computing power. With quantum computers, this could be done far more efficiently, leading to important disease-fighting innovations. In the chemical and materials industries, quantum computing could inform the design of more efficient batteries for electric cars and noncorrosive elements for ships. Quantum computers might also assist in cracking the problem of turning nuclear fusion reactors into a sustainable energy source.

Another promising application area is the field of machine learning. Classical computers training on quantum data—electronic, magnetic, and other information describing the behavior of a quantum system—require enormous quantities of data and processing time. In contrast, quantum computers training on quantum data need exponentially fewer examples to master a task. With such huge gains in efficiency, these machines could be used to learn from and predict the behavior of innumerable chemicals and materials. At present, it remains unclear whether quantum computers will hold an advantage in learning from classical data—such as the text, audio, and video data

underpinning today's AI systems. Yet already, quantum computing is benefiting from advances in classical AI: researchers are using large language models, transformer models, and other AI architectures to help design quantum devices, develop software, and improve quantum error correction.

Of course, it stands to reason that quantum computers should have a natural advantage in applications that are themselves quantum mechanical. Less obvious is what also has been demonstrated—that quantum computers can offer dramatic gains in solving some kinds of non–quantum mechanical problems, such as factorization. Indeed, researchers and mathematicians have discovered 60 algorithms that allow quantum computers to solve problems much faster than classical ones. Some of these speedups are exponential in scale, as demonstrated by the examples above; others are less dramatic but still amount to a significant gain over classical computers.

One intense area of research is the study of optimization. Given a set of variables, optimization seeks to find the most efficient solution and is used by financial planners, shipping logistics managers, and athletic trainers, among many others. Optimization is also central to AI systems. Given how important optimization computations are to the global economy, if even a fraction of them were executed much more quickly and cheaply and with much less energy, the impact would be immeasurable.

FASTER MACHINES, BIGGER RISKS

Quantum computing's possibilities are inspiring, but the technology's current limits are sobering. Getting from today to the advanced systems needed for some of its most promising applications will require integrating deeply complex components and overcoming innumerable challenges. As a result, many of the envisioned applications may still be years away. According to current estimates, for example, a quantum computer that is capable of code breaking will require about 40,000 times as many physical qubits and a five-fold reduction in physical error rates compared with the best current prototypes. Quantum computers that can do simple chemistry calculations are about two orders of magnitude less costly, but they, too, will depend on far more advanced technology.

One measure of the current state of quantum development can be taken from the road map that Google published in 2018. The plan

envisioned six technical milestones that would be required to achieve a full-scale quantum computer: demonstrating that a quantum processor can outperform a classical one on a first task; developing a prototype for a logical qubit; demonstrating an actual logical qubit; building a logical gate for operations between multiple logical qubits; producing 100 logical qubits, which is considered to be a starting point for simple quantum simulation; and producing 1,000 logical qubits for more complex simulations. (A code-breaking computer would require even more advanced capabilities.) Google has achieved its first two milestones, and in December 2024 announced Willow, a new quantum processor that is able to solve in minutes a benchmark algorithm that would take one of the fastest supercomputers today an astounding 10^{25} years to complete. Other organizations—including IBM, IonQ, and QuEra—have published their own road maps to a large-scale error-corrected quantum computer. Chinese researchers, most notably at the University of Science and Technology of China, have achieved Google's first milestone and demonstrated processors with hundreds of qubits. Like other players in the field, Chinese researchers doubtless have other significant developments that have not yet been made public.

To assess the current state of the quantum race, the research arm of the U.S. Department of Defense, the Defense Advanced Research Projects Agency, or DARPA, recently announced a Quantum Benchmarking Initiative to determine whether any quantum computing approach can achieve utility-scale operation by 2033. Although it is impossible to predict the exact pace of future innovation, some researchers have estimated that prototypes of full-scale quantum computers, consisting of perhaps ten logical qubits, may be developed by the end of this decade. Such a feat, together with improved error-correction methods and more efficient algorithms, would bring the world tantalizingly close to quantum simulation.

By current estimates, researchers are unlikely to achieve the first true quantum code-breaking machine—a quantum computer with millions of qubits and adequate error correction—until the late 2030s. Even then, such a computer would take hours to factor a single large number. Still, it is crucial for the United States and its international partners to prepare for this technology now. Networks have been notoriously slow to implement new security standards, despite their long availability. It will take

years to develop, test, and refine a set of quantum-secure standards. The U.S. National Institute of Standards and Technology has been leading an effort since 2016 to develop cryptography standards for a post-quantum world. In August 2024, NIST announced a first set of three classical encryption algorithms as standards ready for immediate use, with instructions for integration into encryption systems and other products. Although this set of algorithms is impervious to all published decryption methods today, it is possible that one or more of them could be vulnerable in the future. Such concerns have taken on added urgency in the wake of new research suggesting that public encryption may never be fully secure against quantum attacks.

Like other new and powerful technologies, quantum computing holds enormous promise, and it also introduces significant new risks. In addition to large-scale data theft, economic disruption, and intelligence breaches, quantum computers could be used for malicious purposes such as simulating and synthesizing chemical weapons or optimizing the flight trajectories of a swarm of drones. As with AI, the possibility of misuse or abuse raises critical questions about who should control the technology and how to mitigate the worst threats. Policymakers will need to determine how to maximize economic and societal gains while minimizing the dangers. Finding the best ways to achieve this balance will require a rigorous debate within civil society and an understanding by the public of the technology's potential gains and harms. There are multiple futures for a world with quantum computers. The best one would see liberal democracies leading both the technology's development and its collective management. A worse one would have the United States and its international partners, through inaction or insufficient actions, cede dominance of the new technology to China and other autocratic countries.

QUANTUM LEAP

Perfecting the quantum computer is a bold, ambitious, and multifaceted project and not one that any company or country can accomplish on its own. Today's early systems already require thousands of specialty parts, tools, and instruments; sophisticated fabrication and cryogenic facilities; and world-class mastery in dozens of technical areas, all supported by billions of dollars of investment in research and development. Tomorrow's systems will be

appreciably more complex. If the United States is to lead this race and, together with its international allies, build the most advanced quantum computing systems, it must allow quantum workers to collaborate across sectors and borders. Effective collaboration can give liberal democracies a significant advantage over more closed, authoritarian countries.

For many companies working on quantum systems today, quantum processors are the crown jewel of their intellectual property and are fabricated in their home country: Google makes quantum chips in the United States, Oxford Quantum Circuits produces quantum chips in the United Kingdom, and Alice & Bob does so in France. In each case, these chips are for in-house research and development; in some instances, third parties are allowed to access early prototypes. As the semiconductor sector has demonstrated, there are geopolitical advantages for any country to maintain the domestic capacity to build a strategic component.

Washington and its partners will need to establish strong quantum-computing supply chains.

But in order to fabricate processors and integrate full computer systems locally, the necessary talent must also be available. This requires collaboration among government entities, industries, and research and educational institutions. Quantum computing companies can support this process by sharing their anticipated workforce needs and providing on-the-job training opportunities. Because the skill sets required for quantum computing are highly specialized, it will not be possible for every country—and may not even be possible for any one country—to develop all the talent needed. Our own work in quantum computing involves collaborations with over 100 academic institutions and industry partners across the United States, Europe, and the Asia-Pacific. The United States and its allies would be wise to implement visa, immigration, and export control policies that allow companies in this critical sector to recruit the most talented scientists, engineers, and technicians. In September, the U.S. Department of Commerce took an important step in this direction by announcing new rules that include a deemed export exemption to facilitate the employment of highly skilled international workers in the United States.

Washington and its international partners will also need to establish strong supply chains for all the subsystems and components that go into quantum computing. Many of the necessary components are and will continue to be produced in disparate locations around the world. Building superconducting qubits, for example, requires many of the same tools that are used in advanced semiconductor-fabrication facilities owned by companies such as Intel and TSMC; these tools are manufactured in France, Germany, the Netherlands, and the United States, among other countries. Cryogenic refrigerators require expertise that is possessed by only a handful of companies, most based in the United Kingdom and the EU. Still other components, such as control electronics and wiring, are designed by specialized companies in Israel, Japan, and Taiwan, as well as in the United States and the EU. Individual countries may attain mastery of different pieces, but like-minded states will need to work together to assemble the full puzzle and keep it out of the reach of authoritarian states.

For quantum computing to achieve its full potential, creative minds from many different disciplines will be needed to develop uses for the technology. There are several early efforts to foster a developer ecosystem, including DARPA's Quantum Benchmarking program, which measures progress toward potential application areas, and XPRIZE Quantum Applications, a three-year, $5 million international competition to generate new quantum computing algorithms for real-world challenges. Gains will come from software developers creating easy interfaces for access, academics and business leaders using these interfaces for the problems most important to them, and consumers and civil society providing input on what they find most valuable.

Like the race to land humans on the moon or to sequence all the genes in the human genome, the successful and safe development of quantum computing cannot be achieved by scientists alone. It will require generational public and private commitments of resources and talent and farsighted international diplomacy. Quantum computers will create extraordinary opportunities for the United States and many other countries around the world. They will also pose new risks, including the potential for abuse or misuse, and possible shocks to the world order. If these dangers can be managed, the potential of quantum computing to accelerate human progress and build a better future could be incredible.