Quantum Technology Challenge: What Role for the Government?

By Paula Ganga
Stanford University
INTRODUCTION

Quantum technology has the potential to reshape the economic and social landscape of the world. The U.S. has already invested significant resources in developing quantum information science (QIS), but more needs to be done as government operations could bear the brunt of the disruptions and possible attacks.

As the U.S. invests the resources to develop this technology and maintain a strategic lead over other countries, cybersecurity—as one of the earliest sectors impacted—will be at the forefront of future developments. Yet the government should not overlook the environmental and sustainability issues that quantum technology entails or the training of a skilled workforce that can proficiently use these technological advances.

This chapter first discusses what quantum technology is and how it could change government functioning. Next, the chapter examines the impact on cybersecurity and cryptography, as well as how quantum might impact environmental sustainability and labor. The last sections of the chapter focus on effective policymaking to make the best use of this emerging technology.

What is Quantum Computing?

Quantum computing makes use of quantum phenomena such as superposition and entanglement to perform faster computations. Quantum physics differs from classical physics in a variety of ways. At the most basic level, understanding quantum starts by distinguishing between the basic unit of analysis in each of these two conceptions of the world.

In classical physics—and the computers based on it—information is stored in binary bits that can take the values of zero or one. In quantum physics, quantum bits (or qubits) can represent both zero and one (or a combination of the two) at the same time. This phenomenon of superposition allows quantum computers to find faster solutions to mathematical problems that currently take classical computers significantly more time and computing capacity.

Comparing complex computational tasks to finding the way out of a maze, a classical computer tries to solve the maze by following every path in sequence until reaching the exit, but superposition allows a quantum computer to try all the paths at once. This drastically reduces the time to find a solution. Increasing the number of qubits results in a dramatic increase in the calculation processing speed. Additionally, various quantum algorithms offer substantial speedups relative to classical algorithms. For
example, Grover’s and Shor’s algorithms each promise a polynomial and an exponential speedup\(^5\) respectively over a classical computer.\(^6\)

The real-world applications of this computational breakthrough can be revolutionizing. In a May 2022 White House National Memorandum, the Biden administration acknowledged the importance of quantum computing for fields as diverse as materials science, pharmaceuticals, finance, and energy.\(^7\) However, that same memorandum sounded the alarm bells for the risks posed by vulnerabilities in existing systems once quantum technology was fully developed. Despite its still mostly theoretical nature, breakthroughs in quantum technology have happened at an accelerated pace in recent years, dramatically hastening the timeline to a fully functioning quantum computer being only 5 to 10 years away.\(^8\)

### Preparing for the Future

In the same memorandum, the Biden administration stated that “while the full range of applications of quantum computers is still unknown, it is nevertheless clear that America’s continued technological and scientific leadership will depend, at least in part, on the nation’s ability to maintain a competitive advantage in quantum computing and QIS.”\(^9\) To this end, the U.S. government has already started to invest substantial efforts and resources in quantum information technology.

### By the numbers

In fiscal year (FY) 2022, the U.S. budget for research and development in quantum computing reached about $900 million, which is double the amount spent in 2019. For example, in the case of the U.S. Department of Defense (DOD), budget requests focusing on quantum-related programs increased by 37 percent between FY2020 and FY2022.\(^10\) According to a report by the National Science and Technology Council Subcommittee on Quantum Information Science, much of this increase in spending was done for activities related to the National Quantum Initiative (NQI) Act, signed into law in 2018.\(^11\)

In FY2023, the U.S. Department of Energy (DOE) received a total of $245 million, including $125 million for five of the DOE-led National QIS Research Centers.\(^12\) The National Institutes of Health’s Office of Data Science received $85 million, in order to implement a new pilot program with the DOE to study the role of quantum computing in biomedical sciences.\(^13\) The National Science Foundation (NSF) received $235 million to continue QIS R&D, including $50 million for research at NQIS Research Centers. The National Institute of Standards and Technology (NIST) funding for QIS reached $54 million.\(^14\) DOD saw several program increases such as $30 million for USAF
Ion Trap Quantum Computing, $10 million for USAF Quantum Network Testbed, $5 million for USAF Secure Quantum Computing Facility, $30 million for university-based quantum materials applied research, $10 million for Army quantum technologies for armament systems, and $1.4 million for quantum computing technologies.\(^{15}\)

**Agility versus redundancy**
The recent growth in QIS R&D is driven in part by NQI activities. Among these activities is the establishment of institutions such as quantum consortia by NIST, Quantum Leap Challenge Institutes through NSF, and National Quantum Information Science Research Centers by the DOE.\(^{16}\)

This flurry of research centers, consortia, and institutes across multiple agencies could be confusing. While this activity is meant to create sufficient opportunities for work on quantum technologies to be developed as widely as possible, it may also create redundancies and function overlap. Congress, in acts mentioning quantum, recognizes the need for urgency in quantum development, but the extent to which government reaches the desired levels of agility and flexibility in developing this technology will depend on how efficiently and effectively these funds reach their target. Moreover, combining government action with initiatives from private actors could create a multiplier effect, but it could also have public and private actors work at cross purposes.

**Cybersecurity and the Cryptography Competition**
The May 2022 White House Memorandum stressed that quantum computing and QIS can create critical challenges in data protection: “A quantum computer of sufficient size and sophistication—also known as a cryptanalytically relevant quantum computer (CRQC)—will be capable of breaking much of the public-key cryptography used on digital systems across the U.S. and around the world. When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most internet-based financial transactions.”\(^{17}\) The computing power of this new technology in the hands of malicious actors could cripple the functioning of the government and the economy. Critical data and infrastructure in the U.S. have been targeted by hackers for years.\(^{18}\) Access to quantum computing could exacerbate this trend if the government cannot quantum-proof its encryption algorithms.\(^{19}\)

**Competition on multiple levels**
At this point, even today’s most advanced classical computers and cryptanalysis techniques cannot easily break current types of encryption. However, a fully functioning quantum computer could break an asymmetric key algorithm in a
Successful attacks against these algorithms could compromise the financial system, critical infrastructure, and military installations.\textsuperscript{21} The dangers of quantum decryption are not only coming from individuals or hacker collectives but also other governments. Much has been written about China having possibly outpaced the U.S. in various applications such as quantum networks and quantum processors.\textsuperscript{22} Additionally, the National Counterintelligence and Security Center identifies quantum computing—along with AI, bioeconomy, autonomous systems, and semiconductors—as one of the strategic technology sectors where the U.S. faces growing challenges from China and an increasingly long list of countries.\textsuperscript{23} Although these five technologies have been singled out as particularly challenging by the U.S. government, experts argue that combining them could be even more dangerous. For example, Quantum Artificial Intelligence—a combination of quantum technology and AI—could compound the disruptive capacity of both technologies.\textsuperscript{24} Any information assumed secure today could be captured and stored to be deciphered later once sufficiently powerful quantum computers are created. Hackers or hostile governments could seize currently encrypted personal or financial data and decipher it retroactively.\textsuperscript{25}

**Sustainable Quantum**

The importance of QIS to fight climate change is one of the most significant advantages experts and government officials mention when justifying continued investment in this technology. The increased computational power of quantum computing can help with tasks as complex as developing new sustainable materials or new sources of renewable energy by:

- Running simulations to test the energy production and efficiency of new materials
- Creating more efficient batteries and cheaper quantum-enabled solar panels
- Improving agriculture and CO2 emissions by streamlining the production of ammonia for agricultural use
- Ramping up carbon capture and carbon sequestration activity
- Improving delivery routes and transportation inefficiencies
- Finding favorable locations for wind and solar farms so they can harvest the greatest amount of natural energy\textsuperscript{26}
These possible benefits compound the already higher computational efficiency predicted for quantum computers compared to classical computers.

According to studies conducted by NASA, Google, and the Oak Ridge National Laboratory, a quantum computer might only require 0.002 percent of the energy consumed by a classical supercomputer to perform the same task with a peak power rating of 25kW. Compared with current supercomputers which sometimes need as much electricity as a small town, a functioning quantum computer can solve problems in a few hours with much less energy.

**Challenges to sustainable physical quantum hardware: cooling and noise**

Currently, the biggest energy consumption of quantum computers comes from the need to keep chips extremely cold in order to perform. The slightest temperature fluctuation can mean that atoms and molecules move around too much, potentially causing a qubit to inadvertently change its quantum state. To this end, temperatures in some parts of the quantum circuit can be 250 times colder than deep space. In addressing this problem, IBM built a super-fridge named Goldeneye to house its largest quantum computers and conduct future experiments. Goldeneye, despite its large size, requires less space than other large-scale dilution refrigerators to house the same amount of hardware. While efficiency gains are important in developing these larger cooling facilities, the cost of building and operating them is still extremely high considering the future expansion of this technology.

Temperature fluctuations are not the only environmental conditions that can impact quantum computers’ functioning. Environmental “noise” can destroy the fragile quantum state of qubits and lead to dephasing. For the longest time, researchers had developed statistics-based models to estimate the impact of unwanted “Gaussian noise” surrounding qubits, but new methods have been developed to deal with non-Gaussian noise and protect qubits from specific noise types.

Many of these solutions have focused on modeling noise such as the “bosonic dephasing channel” model. Both noise and temperature issues show the difficulty in building physical quantum hardware that performs well enough to produce the expected results. Investment in these machines is substantial and much work needs to be done in order to deal with the temperature and noise requirements for a highly sensitive, highly performing quantum computer. In the context of these and other factors that lead to decoherence of the quantum state, a sustainable quantum computing program needs to directly take on these challenges to deliver on the promise of a fully functioning quantum computer in the next 5 to 10 years.
The future is hybrid
To avoid these pitfalls, a host of solutions have been devised. To deal with the exacting requirements for extreme cooling in quantum computing, new initiatives have spurred the development of room-temperature quantum computers. The world’s first room-temperature quantum computer was developed in Germany and is housed at a supercomputing facility in Australia. While the synthetic diamond chip of this computer can only handle 5 qubits compared to over 400 qubits in some of the more advanced quantum computers, because it does not require any cooling infrastructure it can work alongside classical computers and can be more easily integrated into existing systems. This approach is cheaper to build, own, and run, thus bringing quantum technology closer to end users.

In addressing noise, current approaches have focused on modeling the type and source of noise—but considering that this issue also tries to address the impact of environmental conditions on the quantum state of the qubit, a similar hybrid approach should be considered. A hybrid model is one in which the classical computing platform is sitting at one end of the system, and the qubits in the quantum computer at the other. Bridging the two are control processors making hybridization possible, one operating at room temperature to link with the classical computer and one at cryogenic temperatures to monitor the qubits. The two parts of the system divide tasks with the quantum computer handling the hard problems, while the classical systems perform routine tasks. Today many of the quantum systems, from IonQ to D-Wave to Rigetti, are hybrid.

As the U.S. government continues to prioritize both environmental sustainability and quantum technology, investing in hybrid quantum computers should become an important part of the agenda.

The Quantum Workforce
Because quantum computing functions on a completely different paradigm from classical computing both for hardware and software, an important challenge is the expertise required to create working products that leverage this innovation. Right now, only a small very highly skilled elite workforce has the knowledge required to work in this field. In 2021 there was only one qualified candidate for every three quantum jobs available, and the gap continues to persist.

This means that only a small elite workforce has the skills to contribute to these developments and fill jobs in this field. To overcome workforce limitations and democratize access to these powerful systems, many suggest investing more in basic STEM knowledge as early as possible, while another
approach has been to develop ready-to-run quantum software that subject matter experts with no quantum experience can use in hybrid classical-quantum computing systems.41

**Overcoming the talent gap**

Through the National Quantum Initiative Act of 2018, the U.S. has already allocated funding for the development of a quantum workforce. Among the points of this action plan are objectives such as:

- Encouraging the creation of collaborations between industry and academic institutions
- Using and improving existing programs to increase the quantum workforce
- Encouraging academic institutions to consider quantum science and engineering as a different discipline in need of new teachers, curricula, and initiatives
- Starting quantum science education as early as primary schools
- Targeting the wider public so that quantum science knowledge increases at the level of the whole society42

The great educational requirements for this overhaul of the American workforce explain the high number of quantum-focused institutions recommended by the U.S. government and funded through the NQI.

**LOOKING FORWARD**

**Recommendations for Leveraging Quantum Computing**

For the government to fully benefit from the advances of quantum computing, early investment has been crucial as shown by the resources allocated so far. But the roles the government can play in QIS are multifaceted. To make the best of this investment, several roles and policy recommendations stand out alongside existing government policy.
A leader in cybersecurity
In the case of cybersecurity, a two-pronged approach is required. This means not just investment in quantum technology but also in better classical encryption. Right now, hackers routinely exploit vulnerabilities in network encryption and download sensitive data, which could be decrypted later when quantum decryption catches up. With the data already downloaded, accessing this sensitive information will not be hard. Thus, the government needs to switch from being the object of cyberattacks to proactively addressing cybersecurity in both classical and quantum terms. This proposal requires collaboration across a multitude of actors both domestic and international to prevent bad-faith actors from attacking the system—whether hackers or other governments. The U.S. has already hosted an international roundtable in May 2022 with the heads of quantum strategy offices in Australia, Canada, Denmark, Finland, France, Germany, Japan, the Netherlands, Sweden, Switzerland, and the UK. The next step would be to expand this cooperation and create more permanent systems for collaboration.

Supporter of industry initiatives
In the case of quantum sustainability, another two-front approach is recommended. The U.S. government should pursue both increasing efficiency for cooling technology and “noise” reduction in quantum computing, but also developing hybrid quantum computers. This will allow the U.S. to continue housing quantum computers with the largest number of qubits, but also develop smaller hybrid quantum computers for easier integration in the wider economy. Only continued development in both technologies can ensure U.S. “quantum supremacy.”

Quantum innovator
Finally, in the field of quantum education and training, the U.S. government can become an innovator by adding to existing educational initiatives and research centers, taking a new hands-on approach to quantum training on the job. As quantum technology becomes more available and more employees use it, the U.S. government should not rely only on students currently in STEM training. This could leave millions of U.S. workers out of the economic benefits of the quantum revolution. The government instead can take the lead by creating pilot programs to train employees in its own ranks. As the nation’s largest employer, the government can leverage this position to start creating the quantum workforce of the future from within, and expand the training developed through this educational initiative as widely as possible throughout the U.S. economy.
Current debates about whether AI may lead to eliminating jobs show the importance of dealing with the impact of technological progress as soon as possible. To avoid the economic dislocations and inequalities that may accompany a new technology—whether steam power, AI, or quantum—the government can play an active role not only in mitigating the difficult economic consequences, but in shepherding innovation via policy.

Paula Ganga, PhD, is an Assistant Professor of Political Economy at Duke Kunshan University and a Visiting Fellow at Stanford University. She was a Postdoctoral Fellow at Columbia University’s Harriman Institute and the Skalny Center for Polish and Central European Studies at the University of Rochester after completing her doctorate at Georgetown University.

Endnotes
4 In an example provided by Deodoro et al., “two traditional binary bits are needed to match the power of a single qubit; four bits are required to match two qubits; eight bits are needed to match three qubits; and so on. It would take about 18 quadrillion bits of traditional memory to model a quantum computer with just 54 qubits. A 100-qubit quantum computer would require more bits than there are atoms on our planet. And a 280-qubit computer would require more bits than there are atoms in the known universe.” (Deodoro, Jose, Michael Gorbanyov, Majid Malaika and Tahsin Saadi Sedik, “Quantum Computing and the Financial System: Spooky Action at a Distance?” (IMF Working Papers, 2021), 6.)
5 A polynomial speedup is when a quantum computer can solve a problem in time T, compared to a classical computer which would need the longer time T². In the case of an exponential speedup, the classical computer needs time 2¹.  
9 White House, “National Security Memorandum.”


17 White House, “National Security Memorandum.”


Gaussian noise can be compared to white noise coming from the murmuring of a large crowd, whereas non-Gaussian noise features distinctive patterns from a few particularly strong noise sources. See Rob Matheson, “Uncovering the hidden “noise” that can kill qubits,” September 16, 2019, https://news.mit.edu/2019/non-gaussian-noise-detect-qubits-0916.


Kelley, “The White House.”


