



QUANTUM FUTURES: INTERNATIONAL DEVELOPMENT AND THE QUANTUM COMPUTING TRANSITION



USAID
FROM THE AMERICAN PEOPLE

QUANTUM FUTURES: INTERNATIONAL DEVELOPMENT AND THE QUANTUM COMPUTING TRANSITION

Quantum Computing and International Development

This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID) under the terms of contract no. 7200AA18C00057, which supports the Research Technical Assistance Center (RTAC). This report was produced by Abhilash Mishra (Equitech Futures and the Kevin Xu Initiative on Science, Technology, and Global Development, Harris School of Public Policy, The University of Chicago) and Bhasi Nair (Equitech Futures) under the RTAC contract. The contents of this report are the sole responsibility of RTAC and NORC at the University of Chicago, and do not necessarily reflect the views of USAID or the United States Government.

Research Technical Assistance Center

The Research Technical Assistance Center is a network of academic researchers generating timely research for USAID to promote evidence-based policies and programs. The project is led by NORC at the University of Chicago in partnership with Arizona State University, Centro de Investigación de la Universidad del Pacífico (Lima, Perú), Davis Management Group, the Duke Center for International Development, Forum One, the Institute of International Education, the University of Notre Dame Pulte Institute for Global Development, Population Reference Bureau, the Resilient Africa Network at Makerere University (Kampala, Uganda), the United Negro College Fund, the University of Chicago, and the University of Illinois at Chicago.

Suggested Citation

Abhilash Mishra and Bhasi Nair. 2023. Quantum Futures: Making Quantum Computing Work for International Development. Report. Research Technical Assistance Center: Washington, DC.

EXECUTIVE SUMMARY

Quantum computing has the potential to profoundly impact global development over the next several decades. Development practitioners across a wide range of sectors—from applications in digital finance to broader priorities like tech workforce development—must prepare for the risks and opportunities the quantum computing transition may offer.

This report is an effort to synthesize current understanding of how quantum computing may affect the trajectory of global development over the next two decades and proposes how practitioners and decision-makers can respond. We identify key risks of quantum computing that must be addressed proactively by the development community in the short term. We also identify potential opportunities of quantum computing and propose actions to make the most of these opportunities. We hope this report is useful for development practitioners, policymakers, funders, and researchers.

Context

Quantum computing is an emerging technology that seeks to exploit the laws of quantum mechanics to process information with unprecedented speed and efficiency. Given the rate of advancement in quantum technologies over the past few years, experts in industry and academia expect that—in the next several decades, if not sooner—quantum computers will outperform today's most powerful computers by a wide margin. Quantum computers will play an important role in simulating and optimizing complex systems—including in drug development, logistics, and forecasting—with profound economic implications. One of the clearest and most worrisome applications of this computing power is that it could break the existing encryption protocols that keep our information systems and critical datasets safe. This poses a significant national security threat for any country.

Yet like many advanced technologies, quantum technology development mirrors global inequality. The capital costs to build a quantum computer are immense. Only a handful of quantum computers are under development, owned by some of the world's largest technology firms. Wealthy governments, too, are competing for superiority in quantum technologies, and public investments and startup activity in North America, China, and Europe dominate the landscape. Yet, the threats and opportunities posed by the emergence of quantum technologies will be felt globally.

Without concerted intervention in several key areas, this existing global inequality will amplify over time. While the benefits of quantum technologies will accrue to developed countries, the opportunity costs and risks will accrue to less developed countries.

Recommendations

This report focuses on three areas where strategic and foundational interventions today could enable a more inclusive and equitable quantum computing future. These areas—cybersecurity, workforce development, and research and development—are already key priorities for USAID and other organizations in global development. This portfolio could be adjusted to ensure this work takes into account the unique challenges that quantum computing poses. The following recommendations illustrate concrete steps that development organizations, policymakers, and institutions must consider to remain resilient and secure in the post-quantum era:

Cybersecurity: Current encryption protocols used for messaging, financial transactions, and data storage will be compromised with the advent of quantum computers. This threatens existing financial and encrypted messaging systems. Cybersecurity is the sector for which quantum computing will have the most obvious and tangible impact, and USAID and other development agencies should play a role in helping governments and the private sector transition to quantum computing-resistant cryptographic protocols. As this research shows, investments in cybersecurity cannot wait until after the development of functional quantum computers; instead, investments must be made now to be prepared. Our key recommendations are:

- In partnership with relevant technical experts, USAID should develop a “Quantum Risk Audit” protocol and engage governments and non-governmental organizations (NGOs) in low- and middle-income countries (LMICs) to proactively conduct the audits on existing digital infrastructure.
- USAID should establish a “Global Quantum Transition Taskforce” that supports governments and NGOs in LMICs to transition to quantum-safe encryption protocols.
- USAID should strengthen the cybersecurity capacity of the public sector in LMICs by supporting technical experts to work with USAID Missions in partner countries. USAID already supports capacity-building efforts through the [Digital APEX](#) program, and this work should be sustained and expanded to meet the needs of the post-quantum era.
- USAID should work with ministries of technology or digital transformation to promote public awareness of cybersecurity risks from quantum computing in the next decade.

Quantum computing workforce development: Talent required to accelerate progress in quantum computing remains in short supply in both developed and developing countries. However, developing countries will face much stronger headwinds without improvement in science, technology, engineering, and mathematics (STEM) learning outcomes at the secondary and post-secondary levels. Low levels of digital literacy also make citizens in these countries more vulnerable to cybersecurity risks. We discuss how USAID and other development agencies can play roles in building an ecosystem of workforce development, from investing in better STEM learning outcomes to supporting upskilling programs to meet the talent needs of the quantum computing transition. Our key recommendations are:

- USAID should support universities in LMICs to launch new master’s programs in quantum computing and new MS/MBA programs through a new “Quantum Workforce Development” grant.
- USAID should fund pilots to evaluate the effectiveness of bootcamps in upskilling the current STEM workforce for jobs in quantum computing.
- USAID should support awareness campaigns and scholarships that promote the promise of quantum computing to attract talented youth in developing countries to pursue careers in quantum computing and adjacent fields.

Investing in a global quantum computing research and innovation ecosystem: Research and development in quantum computing has been driven by public investments in developed countries and through startup activity predominantly centered in North America, China, and Europe. Combined with the skilled labor gap in developing countries, this has worrying long-term implications for global development. Failing to implement proactive measures to strengthen quantum research and development may significantly exacerbate economic inequality. We discuss how development agencies can support research and innovation in quantum computing by facilitating greater collaboration between researchers in the United States and countries where USAID operates. Existing USAID programs like Partnerships for Enhanced Engagement in Research ([PEER](#)) have been supporting scientists and engineers in USAID partner countries. This can be leveraged to build global partnerships for quantum computing research in developing countries. USAID can also act as an investor for quantum computing startups that focus on key development challenges through funding programs like [Development Innovation Ventures](#). Our key recommendations are:

- USAID should leverage existing USAID programs like PEER to support collaboration between U.S.-based quantum researchers and their LMIC counterparts.
- USAID should provide grants to selected universities in developing countries to launch interdisciplinary programs in quantum computing. The grants can support establishment costs and early faculty hires to attract top talent.
- USAID should fund an annual “Quantum Computing for Development” conference or create such a track at an existing technology and international development conference; this will seed new collaborations between researchers, industry experts, and policymakers.

We begin with a quantum computing overview that is accessible for non-experts. Then we focus on the three priority areas discussed above. We conclude with additional considerations development practitioners should keep in mind and provide concrete recommendations for USAID.

While the trajectory that quantum computing will take in the next decade is uncertain, development practitioners and agencies should make sound investments that can mitigate risks from this new technology and enable developing countries to leverage its potential. Even if quantum computing develops along a different trajectory than currently anticipated, acting on these recommendations will strengthen digital ecosystems in developing countries and will therefore be worth the investment.

TABLE OF CONTENTS

Executive Summary	3
Lists of Tables, Figures, and Acronyms	7
Glossary	8
A Brief Overview of Quantum Technologies	9
The three clusters of quantum technologies	10
Cybersecurity Preparedness for Quantum Computing	14
Timelines for the quantum cryptography break	15
Quantum-resistant cryptography	17
Preparing for the quantum cryptography break	18
Investing in a Global Quantum Workforce	20
The quantum computing talent pyramid	20
Quantum computing workforce for the private and public sector	22
Supporting Research and Innovation in Quantum Computing	23
Public sector	24
The People’s Republic of China, the European Union, and the United States	25
India, South Africa, and Thailand	26
Private sector	26
Quantum Computing and Global Inequality	29
Quantum computing as a driver of economic inequality	29
A quantum computer for low- and middle-income countries	30
Supply chains and manufacturing	31
Raw materials	31
Component manufacturing	32
Potential applications for development	33
Recommendations: Managing Risks and Opportunities of Quantum for Global Development	34
Equipping LMICs for cybersecurity risks from quantum computing	35
Investing in quantum-ready human capital	36
Building research and development ecosystems	36
References	37

LISTS OF TABLES, FIGURES, AND ACRONYMS

Tables

Table 1.	Overview of security protocols and their use	-----	14
Table 2.	Investments in quantum computing globally	-----	23

Figures

Figure 1.	Clusters of quantum technologies	-----	9
Figure 2.	Quantum key distribution	-----	12
Figure 3.	Short- and long-term strategies for post-quantum cryptography	-----	19
Figure 4.	The talent investment pyramid for quantum computing	-----	20
Figure 5.	The talent gap in quantum technology jobs	-----	21
Figure 6.	Private venture capital investments in quantum computing globally	-----	26
Figure 7.	Global distribution of quantum computing startups	-----	27
Figure 8.	The quantum value chain	-----	30

Acronyms

AI	Artificial intelligence
GAVI	Global Alliance for Vaccines and Immunization
LMIC	Low- and middle-income countries
NIST	National Institute of Standards and Technology
NGO	Non-governmental organization
NSA	National Security Agency
NGO	Non-governmental organization
PEER	Partnerships for Enhanced Engagement in Research
PQC	Post-quantum cryptography
RSA	Rivest-Shamir-Adleman
STEM	Science, technology, engineering, and mathematics
USAID	United States Agency for International Development
VPN	Virtual private network

GLOSSARY

Artificial intelligence (AI) – computational models that “learn” from vast quantities of data to perform tasks traditionally associated with human intelligence, e.g., image recognition or text generation.

Cryptography – algorithms or protocols used to secure private communication against access by unwanted parties.

Cybersecurity – tools used to protect computer systems and networks from malicious attacks.

Fault tolerance – the ability and extent to which a quantum computer can function as intended despite the information in individual qubits being compromised due to inevitable interactions with the environment.

Optimization – the selection of the best item among a set of alternatives with regard to a given criterion and some constraints: for instance, if a mail carrier may wish to optimize their mail delivery route with respect to either time or mileage, with the constraint of avoiding highways.

Quantum advantage – demonstrable performance enhancement by using a quantum device to accomplish a task (e.g., a computational problem) as opposed to a classical alternative.

Quantum communications – technologies that exploit the laws of quantum physics to securely convey information across networks.

Quantum computing – an alternative method of computation that exploits the laws of quantum physics to efficiently solve some problems that are difficult to solve with classical computing.

Quantum parallelism – the unique ability of quantum computers to process all possible inputs at once by using qubits in quantum superposition.

Quantum sensing – technologies that exploit the laws of quantum physics to measure physical quantities like time, current, etc., with unprecedented performance (e.g., precision, resolution, etc.).

Qubit – the quantum equivalent of a classical bit that, unlike a classical bit, can be in both 0 and 1 states simultaneously, known as a quantum superposition.

Simulation – computational models that mimic the behavior of real-world systems like enzymes or fuel cells.

A BRIEF OVERVIEW OF QUANTUM TECHNOLOGIES

Information fuels the digital age. The technologies that enable us to handle information—the sensors that gather, the computers that process, and the communication networks that convey information—have advanced at an astonishing rate since the middle of the 20th century. This rapid advance is evidenced by the fact that an iPhone 8 is more than 20 times as powerful as the legendary IBM Deep Blue supercomputer that defeated the then-world chess champion Gary Kasparov in a chess match in 1997 [1].

In recent years, however, the rate of this advance has slowed, as we may be reaching the limits of possibility offered by today's information technologies. At the same time, society's information-related demands are growing exponentially, with unprecedented amounts of big data being generated every second [2]. Alternative technologies that enhance and expand our information-handling capabilities are being developed to meet the requirements of the future.

In the early 21st century, we are witnessing the emergence of a new class of information technologies based on directly interfacing with nature at the quantum level [3-5]. These new quantum information technologies seek to exploit the possibilities offered by the laws of quantum mechanics to gather information with unprecedented accuracy and resolution, process information with unprecedented speed and efficiency, and convey information with unprecedented security, giving rise to three associated clusters of technologies [4,5]:

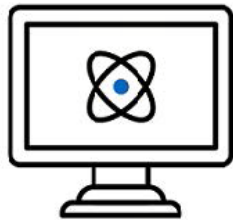
1. Quantum sensing
2. Quantum computing
3. Quantum communications

As these technology clusters develop, talent and investment (both public and private) are being channeled in a quest to secure quantum advantage—a marked improvement in performance over today's information technologies [6,7].

In this section, we provide an overview of quantum technologies, with the bulk of our attention on quantum computing. We start by explaining the peculiar features of the quantum world that allow for novel ways to handle information. We then explore how these features are exploited by quantum technologies to solve real-world problems, along with challenges to scale.

The three clusters of quantum technologies

Figure 1. Clusters of quantum technologies.



Quantum Computing



Quantum Sensing



Quantum Communications



(a) Quantum computers perform computational tasks that can be made easier by exploiting the unique features of quantum mechanics. (b) Quantum sensors make high-precision measurements of physical quantities such as voltage, time, and temperature by using the features of quantum mechanics to mitigate issues that usually limit performance. (c) Quantum communications replace traditional cryptography with protocols that derive their security from fundamental constraints placed by the laws of quantum mechanics.

Quantum computing uses the principles of quantum mechanics to achieve quantum advantage in computing, meaning a marked reduction in the computational resources (time, energy, and memory) required for complex or time-intensive computing tasks [6,9]. In classical computers, the basic unit of memory is the bit, while in quantum computers, the basic unit of memory is the qubit. A bit must be in either one of two states, usually denoted 0 or 1, while a qubit can be simultaneously both 0 and 1 in a quantum mixture known as a superposition. Qubits in superposition permit quantum algorithms to employ quantum parallelism. While a classical program processes a single input to produce a single output, quantum parallelism allows quantum programs to process all possible inputs simultaneously. So, in the case of a “guess-and-check” problem like guessing a password, a classical computer must try many possible inputs sequentially, one by one. On the other hand, a quantum computer can try many guesses at the same time, in parallel. This is one of the defining features that sets quantum computing apart from classical computing.¹

Experts in industry and academia expect developments in quantum computing over the next decades will enable quantum computers to outperform classical computers in addressing a variety of societally and economically relevant problems [4-6,9,10]:

- **Cryptography:** Quantum computers of sufficient scale and reliability—potentially realized as soon as 2030 [8,11]—can be used to break security protocols like Rivest-Shamir-Adleman (RSA) or elliptic curve encryption, which secure much of today’s communication over public and private networks [8,11,12]. However, post-quantum cryptography (PQC) algorithms are already available and only require classical computers to implement [8,12]. Details on PQC and recommendations related to transition to it are discussed in Section 3.

¹ Quantum parallelism is insufficient in ensuring a quantum computer is faster or more efficient than a classical computer. Quantum programs can still only yield a single output, randomly “chosen” from among all the outputs associated with each of the inputs. This means quantum programs are often, in practice, no better than classical programs at accomplishing many computational tasks. However, crucially for some computational tasks, quantum algorithms can be devised to ensure that the output is the one we desire with very high probability. Reading out the result of a computation requires the measurement of qubits, which may not collapse to the right classical bits indicating the correct answer, as the process of measurement and collapse is inherently probabilistic. Quantum algorithms therefore cleverly utilize interference and entanglement to operate on qubits in a manner that maximizes the odds that a measurement of the algorithm’s output yields the correct answer.

- **Simulation:** Classical computers are ill-suited for the study of materials, chemicals, and biomolecules, whose properties are dominated by complex interactions that are difficult to model [13,14]. This makes today's materials and drug discovery a tedious and expensive trial-and-error process, in which simulation can serve only as a rough guide [15]. Quantum computers programmed to mirror the physics of these systems can efficiently predict the properties of new materials and drugs—cutting the time from inception to market by lowering the number of development cycles required [15,16].
- **Optimization:** A wide range of problems, from logistics to portfolio management, involve identifying optimum values of numerous variables under constraints [15]. For a classical computer, solving such problems can become exceedingly inefficient for complex systems. Quantum algorithms provide considerable speed-ups for constrained optimization problems, which can be exploited in the near term by hybrid schemes in which approximate optimizations generated by quantum algorithms are fine-tuned by powerful classical computers [17,18].
- **Artificial intelligence (AI):** From self-driving cars to diagnoses based on medical imaging, predictions based on AI have become increasingly ubiquitous and foundational to the functioning of society [19]. A key bottleneck in the deployment and updating of AI models is the time and computational cost incurred when training these models on thousands of terabytes of data—an issue aggravated by the growing carbon footprint of AI [20, 21]. Quantum computers could offer a solution, as they can, in principle, carry out the linear algebra required to train AI models with considerably fewer computational resources [15, 22].

Over the next two decades, quantum advantage in these archetypal computational problems can add significant value across a range of sectors [9,10], including pharmaceuticals [16], chemicals and materials [15], automotive [17], finance [23], climate change [24], and logistics [10]. However, for all but the most rudimentary applications to be realized [13], quantum computing architecture must undergo significant improvements with respect to [8,9]:

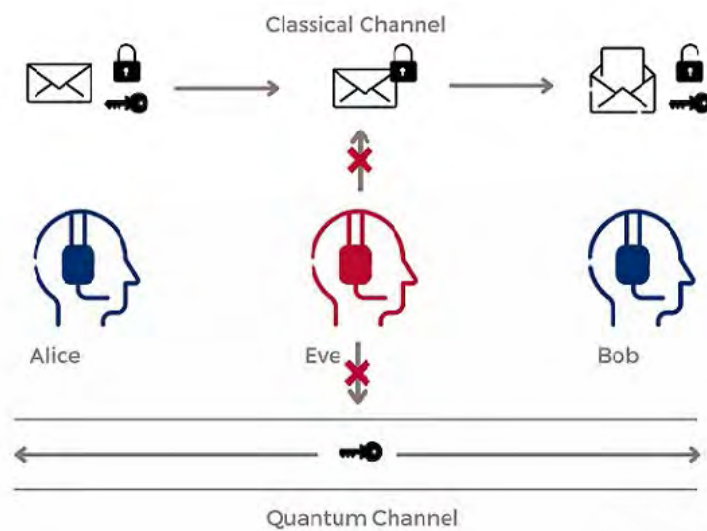
- **Fault tolerance:** Qubits, and the logical operations acting on them, are volatile and sensitive. The slightest interactions with heat, vibrations, or other environmental factors can jeopardize the information stored in qubits. To minimize these effects, quantum computers are typically operated at extremely low temperatures (around -460°F or -273°C) in highly isolated environments. As a result, quantum computers in the near-term are likely to be restricted to quantum data centers that require large amounts of stable power for the maintenance of extremely low temperatures. Even with such measures, today's qubits are still too volatile for mainstream applications. Over the coming two decades, a combination of hardware innovations and algorithmic techniques, referred to as quantum error correction, are expected to address issues of qubit volatility to pave the way for reliable computation.
- **Scale:** State-of-the-art systems currently employ just hundreds of qubits, while applications such as drug discovery will require more than one million qubits. With increasing scale comes greater vulnerability to inevitable interactions with the environment, placing more stringent requirements on the fault tolerance of the quantum computing architecture.


There are no guarantees that quantum computers are necessarily faster or more efficient than classical computers for any computational tasks of practical interest [25]. Classical computing may at any point catch up with or even outperform quantum computers in addressing any of these computational problems. This has in fact already occurred numerous times in the history of quantum computing, when advances in classical computing have caught up with performance from state-of-the-art quantum computers considered to have a definitive quantum advantage [26-28].

Quantum communications refers to new communication protocols that leverage quantum mechanics to strengthen key elements of cryptography [4,7]. Traditional cryptography secures information by forcing hackers to solve difficult mathematical problems that are computationally costly. However, this type of cryptography runs the risk of being rendered ineffective by improved computational capabilities or smarter hacking algorithms. Quantum-based cryptography represents a paradigm shift whereby security is instead based on the basic laws of physics, minimizing the risk of obsolescence. Early efforts in quantum-based cryptography have led to the development of:

- Quantum random number generators that use the inherent randomness of quantum phenomena to generate numbers with unprecedented unpredictability for applications like generating passwords.
- Quantum key distribution [8] for secure communication, as illustrated in Figure 2 below.

Figure 2. Quantum key distribution



 The quantum key distribution uses a quantum channel to share a password stored in qubits between two parties (Alice and Bob in this graphic). This password (or key) is then used to encrypt (lock) and decrypt (unlock) sensitive information conveyed across a classical channel. If an eavesdropper (Eve, in this graphic) tries to tamper with the quantum channel and access the password as it is being shared, the laws of quantum mechanics ensure that either the eavesdropper will fail to do so, or their tampering will be apparent to both sender and receiver.

Quantum communications represents the most technology-ready of the three clusters of quantum technologies. For example, quantum random number generators have already been integrated in some state-of-the-art smart phones. Various telecommunications companies across the world have begun tests of quantum key distribution with the aim of integrating the technology into existing fiber optic networks [29]. Notably, quantum key distribution was integrated into the first-ever quantum virtual private network (VPN) by SK Telecom (based in South Korea) in 2021. Without the stringent hardware or cooling requirements of quantum computers and the ready adaptability to existing fiber optic infrastructure, quantum communications technology can be expected to proliferate more rapidly than quantum computing.

Future advances in quantum communications will likely utilize basic building-block technologies, such as quantum random number generation and quantum key distribution to achieve scalability, range, reliability, and robustness in communication [4]. Such advances would enable quantum networks of distributed quantum processors and sensors to be harnessed by end users in a fully secure fashion. Developments in quantum communications are likely to be crucial to widespread integration of quantum computing in the global economy.

Quantum sensing relies on the sensitivity and scale of quantum mechanical phenomena to achieve measurements of physical quantities with unprecedented resolution, precision, and robustness [30]. In fact, first generation quantum sensing technologies have been in use for decades, namely in atomic clocks for timekeeping and synchronization (used in GPS). Today, spurred by the emergence of quantum computing and communications, a second generation of quantum sensors are being developed to address a trove of applications. In rough order of technology readiness, these include [4,7,30,31]:

- New atomic clocks and accelerometers for improved navigation, synchronization, and regulation
- Sensors for precision electronics and energy applications
- Electromagnetic sensors to be deployed in the body for medical diagnostics
- Cameras and spectrometers for applications ranging from telecommunications to medicine to earth-monitoring
- Thermal and mechanical sensors for civil engineering

In the mid- to long-term, these innovations are expected to yield new metrology standards for effective regulation and standardization that cuts across sectors. Perhaps most importantly, quantum computers are expected to have a distinct quantum advantage in processing and making sense of the quantum information generated by quantum sensors [22]. Thus, even if quantum computers fail to pull away from classical computers with respect to traditional computational tasks like optimization or AI, they may realize economic value through quantum big data generated by quantum sensors. Under this scenario, we can envision advances in quantum communications enabling distributed quantum sensors to be integrated into quantum Internet of Things networks for applications ranging from tests of fundamental physics to climate change monitoring and bioimaging [7].

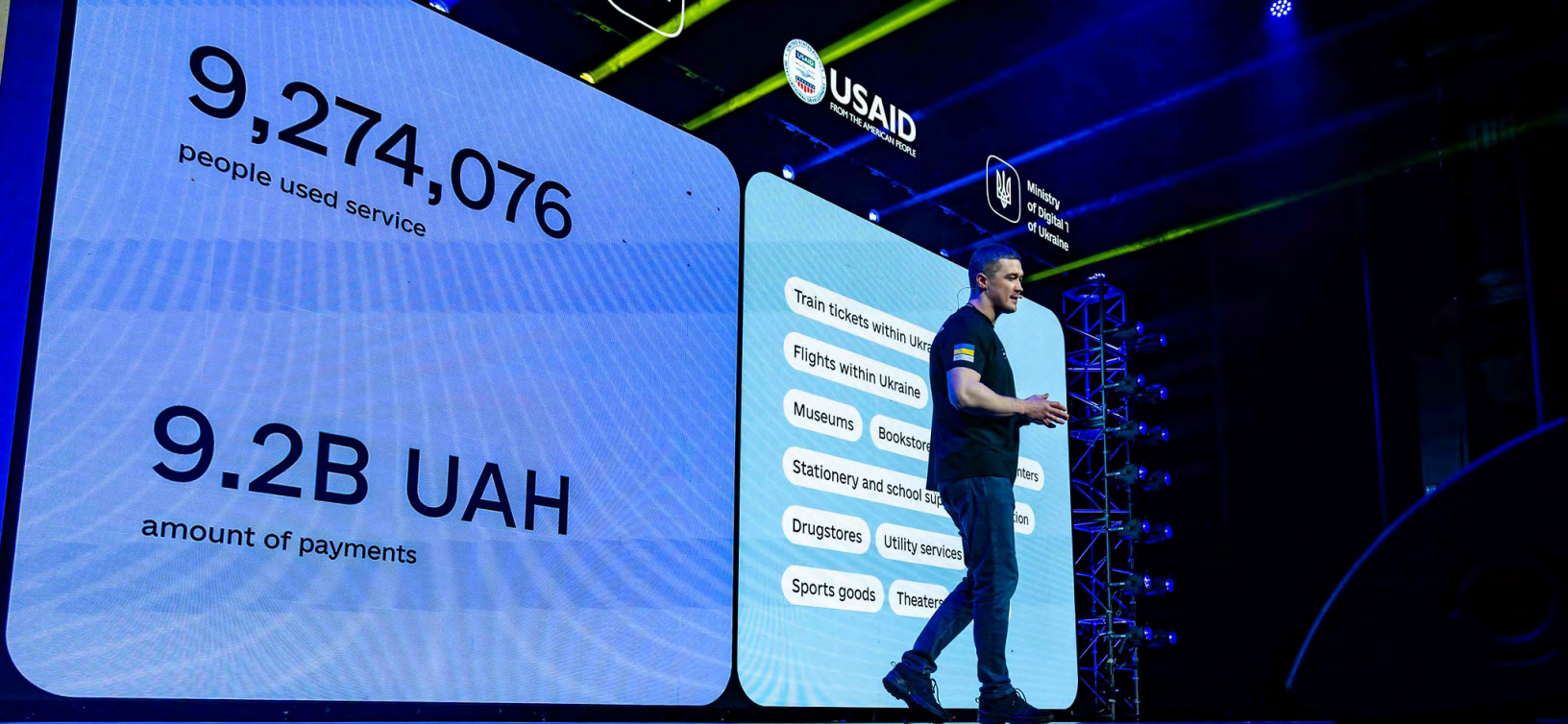


Photo Credit: USAID

CYBERSECURITY PREPAREDNESS FOR QUANTUM COMPUTING

From credit card transactions to personal data, the information conveyed via today's computer networks is secured and validated by **cryptography**, a collection of algorithmic techniques designed to protect sensitive information from malicious actors. These algorithms are based on the principle that certain mathematical problems are very hard to solve, but that if you have the answer, the solution is very easy to verify. For example, guessing a strong password is difficult, but if you have the password, it is very easy to verify that indeed it is right. A typical mathematical problem of this sort, used in traditional cryptography, is prime factorization: breaking a large number into factors that multiply to the large number but cannot themselves be further broken down. Breaking a large number into its prime factors is incredibly difficult, but checking that a set of prime factors does indeed multiply to this large number is easy (a primary school student, with enough patience or a simple calculator, can do the latter).

The result of this is that accessing sensitive information legitimately with a password or key involves merely verifying the solution. Hacking into sensitive information is more challenging—it requires solving the hard problem. At present, malicious actors attempting to break into a cryptographically locked system must try potential solutions to these hard math problems one by one, by trial and error. For today's computers, that could take hundreds of trillions of years to complete, meaning a hacker must resort to finding another vulnerability or giving up entirely.

However, many cryptographic techniques that secure communications over public and private networks are likely to be jeopardized by quantum computing. Qubits in superposition can be used to achieve parallel processing over all possible solutions, and the correct solution among these can be determined with high probability by cleverly engineered quantum algorithms. The following common security protocols—deployed in sectors ranging from e-commerce to health care—are at risk of being broken by quantum computers [8]:

Table 1. Overview of security protocols and their use.

Security protocols	Use
Rivest-Shamir-Adleman (RSA)	Encryption of emails, messages (e.g., WhatsApp) and digital transactions
Diffie–Hellman (Key Exchange)	Establish secure connection between user and, e.g., a private network (VPN), an online banking system, an email server, etc.
Digital Signature Algorithm (DSA)	Generate digital signatures to authenticate messages, ensure their integrity, and prevent repudiation by the sender
Elliptic Curve Digital Signature Algorithm	
HTTPS/TLS	Secure traffic over the Internet

Applications built on top of these bread-and-butter protocols include VPNs, Tor, smartcards, most Wi-Fi security, blockchain technologies like cryptocurrencies, and many two-factor authentication systems. Crucially, these security protocols are generally protected as long as quantum computers lack the scale and reliability to breach them, and the most powerful quantum computers today are still much too simple to crack most cryptographic techniques.² Therefore, **when can we expect the quantum cryptography break?**

Timelines for the quantum cryptography break

There are four possible timelines for the quantum cryptography break:

- **It has already happened:** The quantum cryptography break may have been achieved by a major country's government (likely the United States) in secret—key advances in cryptography like RSA were kept secret by the governments of the United States and the United Kingdom for several years [8]. Alternatively, an algorithmic breakthrough at any point could make current quantum computers sufficiently powerful. Claims of such breakthroughs have been made [33], but none have been verified, and they have been largely met with skepticism [34].
- **It will happen in the near-term (~3–5 years):** Roadmaps set out by governments [35] and major corporate players in the quantum computing space [10] indicate that issues with reliability and scale will be resolved over the coming decade, culminating in the emergence of quantum computers with practical applications before 2030. Timely attainment of corporate benchmarks in the recent past³ can be taken as evidence to support the viability of these projections.
- **It will take a decade or more:** A 2019 survey of academic experts indicated 2035 to be the average year by which experts predicted quantum computers will crack 2048-bit RSA [36]. A 2020 study found the probability of quantum computers cracking 2048-bit RSA before 2039 to be less than 5 percent [37]. In short, the dominant narrative among academics places the quantum cryptography break in the mid to late 2030s (or later).

² A quantum computer running the quantum algorithm for prime factorization (Shor's algorithm) would likely need tens of millions of qubits to crack a 2048-bit RSA key [8]. The most powerful quantum computer developed to date has just 433 qubits [32].

³ For example, Honeywell's successful demonstration of ultra-high fidelity 2-qubit gates in 2021 [10].

- **It will never happen:** Until recently, quantum computers have been largely an academic curiosity. Their practical uses have yet to be developed. However, our current understanding of both physics and computer science indicates the quantum cryptography break is inevitable. As theoretical computer scientist Scott Aaronson aptly states [38]:

“ “[f] scalable quantum computing were proved to be impossible, that would excite me a thousand times more than if it were proved to be possible. For such a failure would imply something wrong or incomplete with our understanding of quantum mechanics itself: a revolution in physics!”

Of these, the 10+ year horizon projected by the academic narrative is the most likely, followed by the three-to-five-year horizon projected by the dominant industry narrative. There are three potential scenarios for the proliferation of quantum computing capabilities:

1. **The capabilities of quantum computing remain in government hands:** Present quantum computing architectures are extremely expensive and based on qubits that are far from reliable. In addition, today's qubits typically require substantial infrastructure for extreme cooling and environmental isolation. Due to these severe hardware limitations, building a quantum computer at scale is likely to require tens to hundreds of billions of dollars. In the absence of major hardware advances that significantly reduce costs, it is possible that quantum computers capable of breaking cryptography are developed only by major governments such as the United States, China, and the European Union within a few years of each other. Under this scenario, these governments could protect and severely restrict quantum computing power to limit the possibility of malicious attacks that could compromise national security. In the United States, strong cryptography has been historically considered “munitions” and covered by the Arms Export Control Act of 1976 [8]. Thus, a scenario akin to the development of nuclear weapons may be envisioned, with international policy shaped to actively minimize the prospect of new entrants to the “quantum club.” Once quantum computing becomes accessible to corporations and individuals, governments may outlaw the use of certain algorithms. This may be analogous to how commercial printers, scanners, and copy machines are (by law) pre-programmed to prevent the production of counterfeit currency [8].
2. **Use by large corporations:** United States-based technology companies such as Google, Microsoft, and IBM have invested heavily in proprietary efforts to translate fundamental research into prototype quantum computers with early commercial uses [10]. If this trend continues, it is possible that these and other major corporate players may develop quantum computers capable of breaking cryptography. In this scenario, cloud-based access to quantum computing resources may be prohibitively expensive for mainstream use, and national laws may restrict access to pre-authorized organizations, with governments being some of the largest customers [8].
3. **Mass proliferation:** Mass proliferation of quantum computing may have already begun. For instance, Quantinuum, a private company formed from the merger between Honeywell Quantum Solutions (based in the United States) and Cambridge Quantum Computing (based in the United Kingdom), offers cloud-based access to limited quantum computing resources for quantum chemistry simulations [39]. Early applications will drive further capital investment, while a quantum computing market emerges linking steadily growing quantum computing resources to end users across diverse sectors [10]. In this scenario, markets for quantum computing-resistant and even quantum computing-based cryptography should develop in parallel and have reached considerable maturity by the time of a quantum computing cryptography break.

The high capital costs and large lead times associated with building quantum computers at scale, along with inevitable protectionism around intellectual property, will most probably physically confine quantum computers to a handful of government and corporate data centers over the coming two decades. The dominant industry narrative suggests that mass proliferation of quantum computation via cloud-based access is likely to occur in tandem. However, the quantum computing capabilities of some governments may precede cutting-edge reports from industry and academia by several years. If so, these governments may achieve crypto-threatening quantum computing well before mass proliferation. Historically, attempts to restrict strong cryptographic capabilities by national governments have managed only to delay inevitable mass proliferation [8]. **Thus, prudence dictates that governments, corporations, and organizations across the world should prepare for the quantum cryptography break as if mass proliferation of such capabilities is likely to take place in the coming decade.**

Quantum-resistant cryptography

Fortunately, quantum-resistant cryptographic techniques⁴ are already well known and can be implemented on classical computers. While some of these techniques are made weaker by the parallel processing capabilities of quantum computers, their intrinsic mathematical structure only permits modest gains⁵ for attacks using quantum algorithms: the equivalent of doubling the length of a password is thought to nullify any gains from a quantum computing attack [8].

The United States National Institute of Standards and Technology (NIST), in coordination with the National Security Agency (NSA), has historically held contests to evaluate novel cryptography proposals to replace existing, at-risk techniques [8]. Winners of these NIST/NSA contests have gone on to become the official cryptography standards for the United States government. By virtue of the size of the economy of the United States and the government's clout as a buyer in computing hardware and software markets, these standards have been adopted around the globe via the Common Criteria Recognition Arrangement, adhered to by much of the developed world as well as by other countries, including India, Pakistan, and Malaysia.

The NIST Post Quantum Cryptography Standardization Process contest was launched in February 2016, drawing 82 initial submissions [40]. The contest is now in its fourth round. NIST announced four algorithms selected for standardization⁶ in July 2022. Of four more being considered, up to two will be selected for standardization. New draft standards for winning algorithms are expected to be reviewed, finalized, and communicated through NIST Federal Information Processing Standards publications before the end of 2024.

4 For example, symmetric or lattice-based ciphers and newer hashes like SHA-2 or SHA-3 of sufficient size

5 quadratic speed-up, as opposed to exponential for RSA, for instance.

6 One for public-key encryption/key establishment mechanism and three for digital signatures

Preparing for the quantum cryptography break

The quantum cryptography break should be seen as a Y2K⁷-type event [8], with the crucial difference that the precise date of the crisis is not known. In hindsight, Y2K is remembered as overly hyped, but this is precisely because of the years of planning and updating systems that preceded the turn of the millennium. Managing the looming quantum cryptography break will require similar planning and system updating, with additional urgency stemming from the uncertainty of when the break will occur.

The urgency of the transition to quantum-resistant cryptography will be dictated by [11]:

- 1. Organizations' value-at-risk:** Governments, financial institutions, and any corporations with proprietary trade secrets may stand to incur significant, even catastrophic losses (financial or otherwise) if vital secrets are accessed by quantum attacks.
- 2. Shelf life of sensitive data:** Many classified documents pertaining to issues of national security can be intercepted in their encrypted form now and decrypted using a quantum computer within the coming two decades, well in advance of their intended date of declassification. Likewise, personal information about individuals held by hospitals, banks, insurance companies, and various social media/technology companies can remain sensitive well beyond the scope of the individual's lifetime. The mere threat of any intercepted personal information being decrypted later by a quantum computer can compromise privacy and undermine trust in these institutions and the services they provide.
- 3. Life cycle of systems/products:** Many physical systems and their associated software are likely to still be in use when the quantum cryptography break occurs. High costs and regulations often translate to long lifetimes for various government systems, meaning that the development and deployment of these systems must already incorporate quantum-resistant cryptography. Likewise, in the private sector, modern cars with high connectivity must meet security standards to protect personal information—a car in development today is likely to be on the road even in the 2040s. This means any remote software updates can be susceptible to quantum attacks.

Thus, organizations with high value-at-risk, long data shelf lives, and long system/product life cycles should start the transition to post-quantum cryptography immediately.

Though quantum-resistant cryptography remains untested (due to the absence of sufficiently powerful quantum computers), it remains the most viable bridge between today's mainstream cryptography and the quantum-based cryptography of the future. Thus, organizations and applications with less stringent performance/budgetary constraints should begin preparations for adopting the anticipated algorithmic standards to be published by NIST. This might involve preparations to retrofit systems with NIST's PQC standards by reserving computational and financial resources as needed, ensuring modularity of security architecture, planning critical software and hardware updates that minimize operational disruption and associated costs, and making vital connections to PQC suppliers, regulators, and other key actors [11]. More proactively, since NIST has identified the algorithms it plans to standardize, these solutions can already be implemented in a crypto-agile manner, to minimize costs associated with adjustments required to meet finalized standards [8].

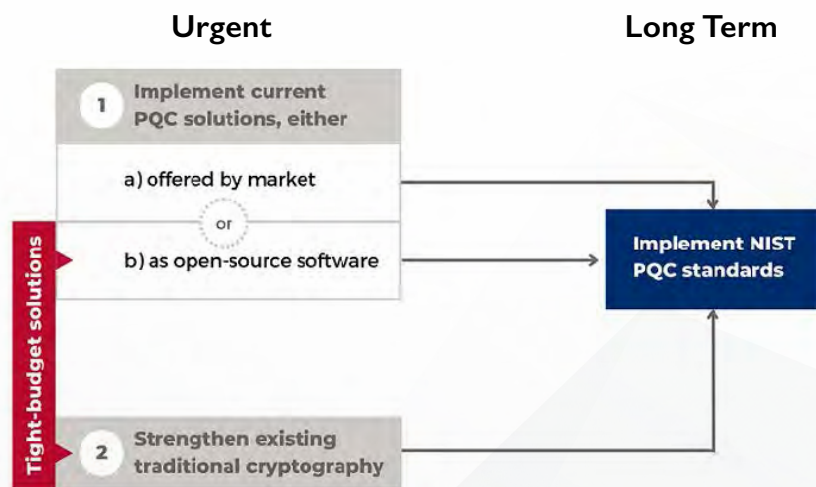
⁷ Calendar year 2000


Due to the inherent uncertainties around the quantum cryptography break, adopting market-based implementations of PQC may be the safest option for most organizations (Figure 3). However, post-quantum cryptography currently makes up just 2 percent of the global cryptography market, meaning that prices remain high [11]. Nevertheless, as NIST’s 2024 standards ratification deadline approaches, the PQC market can be expected to take off, with some analysts projecting a doubling of annual revenue over the next five years⁸ [41]. Thus, a decrease in costs and improvements in performance can be expected for PQC as the market grows.

Adoption of NIST’s post-quantum cryptography standards may be prohibitively expensive for organizations with limited resources or may severely compromise performance/latency for high-traffic applications involving many interconnected devices, such as instant messaging. Under such budgetary or performance constraints, traditional security protocols must, at minimum, be strengthened. For example, moving from RSA-1024 to RSA-2048 encryption (the conceptual equivalent of doubling the length of passwords), is likely to buy one to three years of security [11]. More concretely, adopting the protocols in the NSA’s Commercial National Security Algorithm Suite [42] can ensure systems are secured in the near-term against any initial advances in quantum computing⁹ [8].

Alternatively, organizations with limited resources can look toward open-source libraries of PQC software,¹⁰ as compiled via projects like Open Quantum Safe [43]. Soon, we expect resources and talent diverted to projects like this to grow as the specter of the quantum computing cryptography break looms ever larger. Investing in nonprofit/charity organizations involved in legal/financial aid, advocacy, and governance of open-source PQC can ensure the availability of both robust cryptography solutions accessible to all and the cultivation of a global talent pool required to implement them.

Figure 3. Short- and long-term strategies for post-quantum cryptography.



 Ideally, organizations begin to implement existing PQC solutions offered by the market in a crypto-agile manner as soon as possible. Under budgetary constraints, implementing open-source software may prove to be an economical alternative but will still incur some of the inevitable costs associated with migration to PQC solutions. At the very least, organizations should strengthen existing traditional cryptography, which may buy a few years’ more time to migrate to PQC solutions. In the long run, we expect NIST PQC standards will replace much of traditional cryptography, and organizations should expect to have to migrate to PQC in the coming decade.

⁸ ABI research estimates that PQC revenue of US\$196 million in 2022 will jump to about US\$395 million in 2027 [41].

⁹ Public key algorithms in the CNSA 1.0 suite are vulnerable to quantum attacks, while digital signatures, hashing, and symmetric ciphers are considered quantum-resistant [8,42].

¹⁰ These libraries include both PQC algorithms as well as prototype integrations into traditional protocols and applications (e.g., TLS).



Photo Credit: Bobby Neptune for USAID

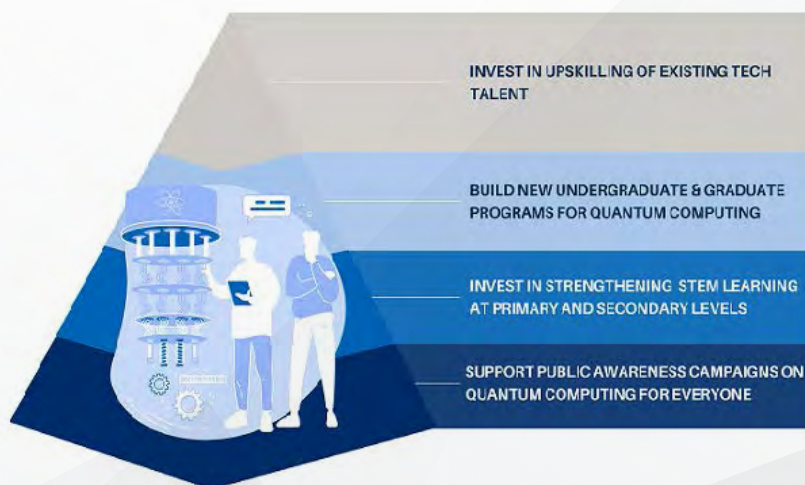
INVESTING IN A GLOBAL QUANTUM WORKFORCE

The quantum computing talent pyramid

The biggest obstacle to overcoming the talent shortage in quantum computing in the coming decades will be inadequate STEM education infrastructure at the secondary and post-secondary levels. This includes lack of specialized degree programs or curricula for quantum computing at the post-secondary level. Even if governments are able to invest in a small number of talented individuals to fill talent gaps, the lack of basic digital literacy in the larger population will exacerbate economic inequality within countries, to say nothing of inequality between high-income countries and LMICs. Poor digital literacy also makes citizens more vulnerable to risks from quantum computing, such as cybersecurity breaches.

It is imperative that developing country governments and development agencies like USAID invest in scientific talent in a multipronged manner. We recommend USAID conceive of investing in talent as building a pyramid. This means investing in a base awareness of quantum computing among the broader public, building up the pyramid by strengthening the teaching of computing skills in schools and universities, and at the top of the pyramid, investing in increasing the skill sets of existing tech talent.

Figure 4. The talent investment pyramid for quantum computing.



In the 2018 book [Leapfrogging Inequality: Remaking Education to Help Young People Thrive](#), the authors paint a grim portrait of the inequality in educational outcomes between developed and developing countries [44]. The book suggests an estimated 825 million children—half the global population under the age of 15—will reach adulthood without foundational language and mathematical skills expected of a secondary-level education. The authors forecast it will take some countries more than a century to achieve the educational outcomes observed in developed nations. School shutdowns and learning loss due to the COVID-19 pandemic are likely to exacerbate such inequalities in educational outcomes [45].

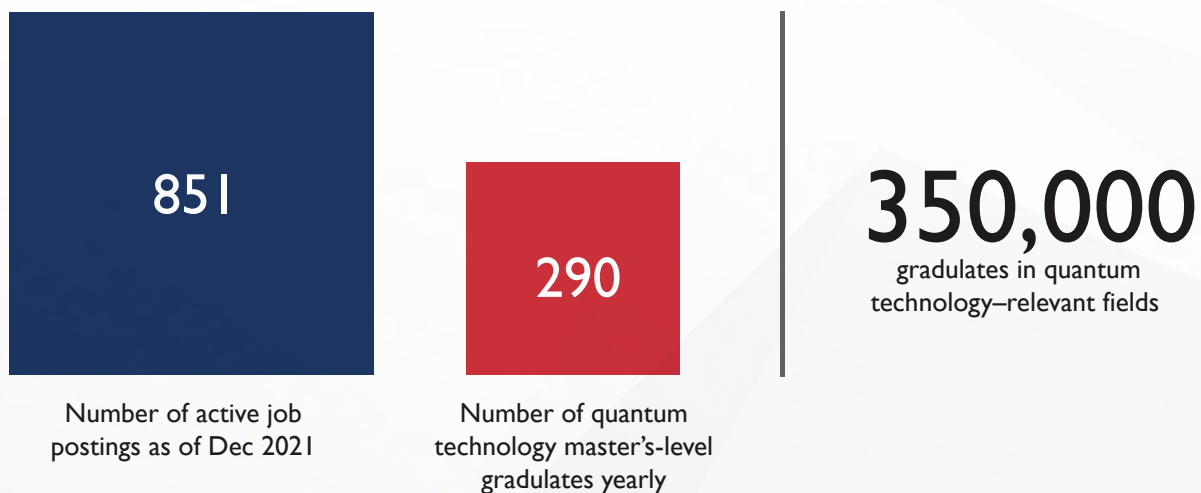
As startling as these estimates are, they do not begin to address the challenges with developing the advanced STEM skills required for the quantum workforce. Workers with such skills are in short supply globally, even in developed countries. For instance, a recent report by global management firm McKinsey & Company found that demand for experts with advanced degrees in quantum computing is outpacing available talent. The number of active job postings in the field in December 2021 outstripped qualified applicants by 3 to 1 (Figure 5) [46]. The report predicts that because of such talent deficits, by 2025, fewer than 50 percent of open quantum computing positions will be filled in developed countries.

This gap poses a unique challenge and opportunity for developing countries. By investing strategically in improving higher education outcomes through specialized graduate programs, developing countries can leverage their large demographic dividends to benefit from the quantum transition. However, if they fail to make these investments, they are likely to miss out on economic benefits, leading to greater tech-driven economic inequality between high-income countries and LMICs.

Figure 5. The talent gap in quantum technology jobs [46].

The number of jobs postings outstrips qualified talent by as much as three to one...

... but upskilling graduates in related disciplines can help close the gap.



Though the supply of quantum technology talent lags demand, the gap can be addressed by drawing from the far bigger pool of master's-level graduates in fields relevant to quantum technology.

Quantum computing workforce for the private and public sector

Current talent for quantum computing companies is drawn from PhDs in quantum physics and engineering. Graduate and undergraduate degrees offering a specialization in quantum computing have yet to become mainstream.¹¹ Industry observers have suggested that establishing new degree programs in computing, quantum physics, and engineering are critical to closing talent gaps in the United States. Developing and offering similar interdisciplinary degree programs in developing countries is also essential to beginning to bridge the talent divide. In India, for example, such programs could be offered in collaboration with the Indian Institutes of Technology/National Institutes of Technology. In South Africa, similar collaboration could result in program offerings at the African Institutes of Mathematical Sciences in Cape Town.

The United States government has also recognized the need to attract top quantum computing talent to remain competitive with the People's Republic of China [47]. Investing in capacity-building for quantum computing through new undergraduate and graduate programs can open a large pool of talent for companies in the United States (currently, immigrants to the country account for more than half of all STEM workers with PhDs [48]).

Finally, industry experts in quantum computing argue that more than technical expertise will be needed in a post-quantum economy. One expert we interviewed¹² highlighted the importance of generalist business training that can help talent in the private sector identify new opportunities for using quantum computing in business. He also emphasized the importance of strong scientific communication skills, which allow quantum computing engineers to interface with business development experts, product designers, and marketers—all essential to building a robust quantum ecosystem. Existing STEM undergraduate degree programs in developing countries tend to emphasize technical training, often eschewing crucial communication and collaboration skills. For developing countries to compete in the future quantum economy, they will need to reimagine the way STEM is taught in their university systems.

The public sectors in both developing and developed countries face increasing challenges in attracting quantum computing talent. Governments around the world will need experts in quantum computing to help secure financial systems and encrypted messaging systems critical to national security. But given the scarcity of skilled professionals proficient in quantum computing, governments will struggle to compete for talent with private firms offering significantly higher salaries. Governments will need to develop novel incentives to attract essential talent. One strategy is to build up programs like a “National Quantum Corps” for early-career professionals to spend a short time working in public service. USAID could leverage its existing science fellowship programs (like the [AAAS Science & Technology Policy Fellowship](#)) to provide quantum computing expertise to developing countries where local talent is hard to find. This could come in the form of short public-private partnerships where quantum computing companies “loan” talent to the government in return for tax breaks or other incentives.

¹¹ Out of the 176 quantum research programs at universities worldwide, only 29 provide graduate-level degrees in quantum computing. [46]

¹² Dr. Mark Jackson a business development lead at Quantinuum, a leading quantum computing software company that grew out of Honeywell.



Photo Credit: David Rochkind, USAID

SUPPORTING RESEARCH AND INNOVATION IN QUANTUM COMPUTING

The largest players in funding the development of quantum computing technologies so far are governments. Given the national security implications of quantum computing technologies, developed countries have begun to invest heavily in quantum computing. Globally, governments have announced plans to invest more than US\$31 billion in quantum computing technologies¹³ [5]. Private sector funding, fueled by venture capital investments, has also exploded over the past five years [49]. However, investments in quantum computing by the governments of the United States, the European Union, and China dwarf those of the public sector funding in all developing countries combined. This poses a grave challenge, and over the next two decades may lead to growing technology-driven inequality. For example, quantum computing has the potential to transform manufacturing. Underinvestment by LMICs in quantum computing can make it difficult for their manufacturing sectors to remain globally competitive. Development agencies must flag these investment trends and design interventions to build a more equitable quantum future.

¹³ Lack of transparency in research and development expenditures by countries such as China (and to a lesser extent Japan) makes precise estimates challenging [10].

Public sector

Government engagement in the development of quantum computing technologies falls into four categories, according to the Canadian Institute for Advanced Research's Report on Global Policies for Quantum Technology [35].

- **Countries with coordinated national strategies for quantum technologies** include:
 - Global economic powers China, major European Union member states France and Germany, the United States, the United Kingdom, and Japan, which have each allocated more than US\$1 billion of public funds to quantum technologies
 - Other high-income countries, notably Israel and Singapore
 - Middle-income countries, notably Russia and Iran (upper-middle) and India (lower-middle)
- **Countries in the process of developing a quantum strategy**, notably:
 - Canada, with perhaps the biggest per capita public spending on quantum technologies to date
 - Upper-middle-income countries such as Thailand and South Africa
- **Countries that have sponsored or endorsed significant initiatives but have yet to develop a national-level strategy**, including several European Union member states and periphery countries such as Norway and Switzerland, Australia, and the United Arab Emirates.
- **Countries participating in international partnerships**, mostly smaller European Union member states such as Belgium, Croatia, and Turkey.

There is little consensus on the estimates for past and projected spending on quantum computing across all countries. Still, it appears the bulk of government-funded research and development in quantum technologies is concentrated in China and in countries that are members of the Organisation for Economic Co-operation and Development, which account for the vast majority of all public funds allocated to the technologies. Of the others—Russia, Iran, the United Arab Emirates, India, South Africa, and Thailand—the latter three may serve as early, illustrative case studies for quantum technology policy in LMICs.

Table 2. The talent investment pyramid for quantum computing¹⁴

Country	Private Sector Investment (as of 2022)	Government Spending (as of 2022)	Projected Government Spending	Estimated Total
China	\$280 million	\$9.7 billion	Not Available	\$10.0 billion
European Union	Not Available	\$1.1 billion	\$7.5 billion	\$8.8 billion
United States	\$3.7 billion	\$2.9 billion	\$844 million	\$7.4 billion
United Kingdom	\$890 million	\$1.0 billion	\$3.1 billion	\$5.0 billion
Germany	\$100 million	\$1.9 billion	\$1.2 billion	\$3.2 billion
Canada	\$700 million	\$748 million	\$270 million	\$1.7 billion
Japan	Not Available	\$1.1 billion	\$607 million	\$1.7 billion
France	\$420 million	\$565 million	\$565 million	\$1.6 billion
Australia	Not Available	\$311 million	\$725 million	\$1.0 billion
Netherlands	Not Available	\$853 million	Not Available	\$853 million
Russia	Not Available	\$790 million	Not Available	\$790 million
India	Not Available	Not Available	\$730 million	\$730 million

¹⁴ <https://www.csis.org/analysis/quantum-technology-applications-and-implications#h2-quantum-research-is-global>

The People's Republic of China, the European Union, and the United States

Quantum technology strategy and policies in the People's Republic of China, the European Union, and the United States are driven by several common elements, including [4,35]:

- **Technological sovereignty:** Both China and the European Union have prioritized local development of universally programmable quantum computing capabilities—an emphasis mirrored in other emerging technologies, like nuclear fusion [50] and AI-based large language models [51]. In the case of quantum computing, calls for technological sovereignty are likely responses to the domination of United States-based technology companies in translating fundamental quantum research into viable prototypes through in-house, capital-intensive research and development.¹⁵ As a result, both China (US\$15 billion) and the European Union (US\$7.2 billion) have committed significantly higher public funding toward quantum technologies research and development compared to the United States (~US\$2.6 billion¹⁶) [5].
- **Financing startups:** The European Union has prioritized securing local venture capital to counter the draw of Silicon Valley for growth-stage startups. China has similarly emphasized expanding investment and nurturing promising early-stage startups through state-owned funds and initiatives such as the “Little Giants” program that provide grants, subsidies, and tax cuts [53].
- **Building key infrastructure:** The European Union has emphasized the need for major infrastructure projects to scaffold the transfer of quantum technologies from “lab to fab to market,” presumably in part as a response to China’s arguable comparative advantage in quantum communications and its fiber optic and satellite infrastructure. The United States has more recently directed funds into its Quantum Network Infrastructure project through the CHIPS Act, with allocations of US\$100 million annually over the next five years [52].
- **Securing intellectual property:** The acceleration of quantum technology patents across computing, communications, and sensing in China, the European Union, and the United States, over the last five years is the direct result of initiatives intended to scaffold technology transfer and incentivize private sector involvement. However, experts have raised concerns that overprotection could stymie healthy competition [54].
- **Governments as conveners:** China, the European Union, and the United States have introduced numerous initiatives to bring together stakeholders from across the technology development cycle to facilitate “ecosystems” of quantum innovation, notably through research networks, large-scale collaborations, and industry-academia consortia.
- **Strengthening supply chains:** The establishment of robust supply chains to support the accelerating demands of quantum technology activity has been a priority for China, the European Union, and the United States. Some countries have made large investments in specific physical platforms for quantum computing (e.g., silicon-based quantum computing in France), presumably seeking to leverage established supply chains and competitive advantages.
- **Cultivating human capital:** China, the European Union, and the United States have prioritized developing high-level quantum technology talent and accelerating research and development and innovation in the field. Such programs are developing a growing workforce knowledgeable about how to use the technologies and the value they offer.

¹⁵ The volume of internal funding for quantum technology projects within large technology companies is difficult to ascertain due to lack of transparency.

¹⁶ Includes the latest government spending as summarized in references [4,52].

India, South Africa, and Thailand

India has allocated approximately US\$1 billion between 2020 and 2024 devoted to a comprehensive and substantial quantum technology strategy that includes [35,55]:

- Prioritizing Indigenous quantum computing capabilities.
- Creating research parks and quantum computing hubs to bring together all phases of the technology development cycle, from basic research to startup incubation.
- Initiating large-scale international collaborations to lay the groundwork for vital infrastructure in both quantum computing (with Finland and Russia) and quantum communications (with Israel and BRICS countries). The Quad partnership, which includes India, has underscored quantum technologies as a key area of collaboration [56]. More recently, India and the United States entered a partnership through the initiative on Critical and Emerging Technology [57] that created a joint Indo-US Quantum Coordination Mechanism with participation from industry, academia, and government to facilitate collaboration between researchers and industry in both countries.
- Focusing on cultivating human capital at the university and postgraduate levels, to ensure a steady flow of talent.

South Africa has set up a working group to define its quantum computing strategy, while tangible activity has included [35]:

- A partnership between IBM research at Johannesburg and the University of Witwatersrand, giving IBM's Q Network access to the 15 universities in the African Research Universities Alliance.
- Collaboration with other BRICS countries on the development of quantum computing communications infrastructure.

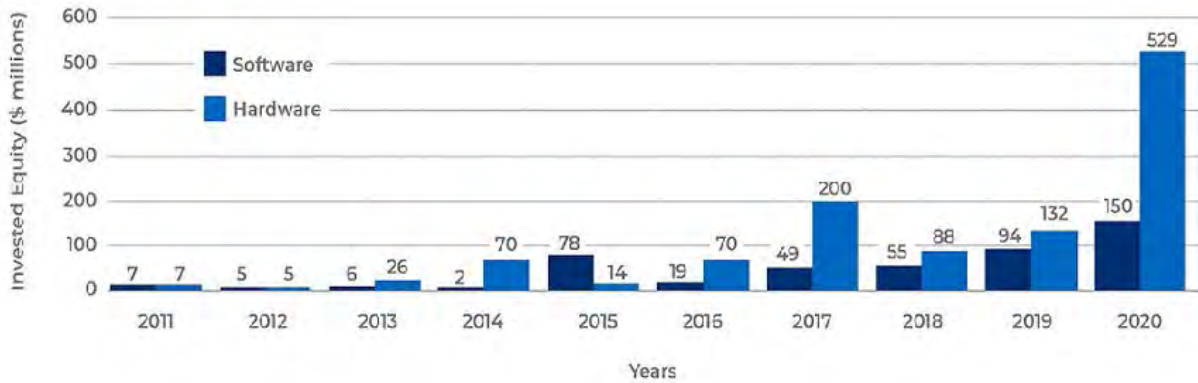
Thailand has announced the allocation of nearly US\$6.6 million to the development of quantum technologies. Plans to launch a National Institute for Quantum Technology in the near future are under discussion [35].

In comparison, the quantum technology strategies of other LMICs studied in the preparation of this report are less mature.

Private sector

By the end of 2021, more than US\$4 billion of private investment had been channeled into quantum technology startups, roughly 80 percent to English-speaking nations (mainly the United States, the United Kingdom, and Canada) where roughly 50 percent of all quantum startups are based [5]. When it comes to quantum technology patents, China's government policies and Japan's early adoption of quantum technologies by industry have led both countries to dominate the landscape. Between 2000 and 2021, 54 percent of quantum technology patents were held by Chinese companies and 15 percent by Japanese firms [5,54]. The European Union has both the highest number and per capita concentration of quantum technology talent (231 patents per million people) and is the base of operations for more than a quarter of all publications on quantum computing [5].

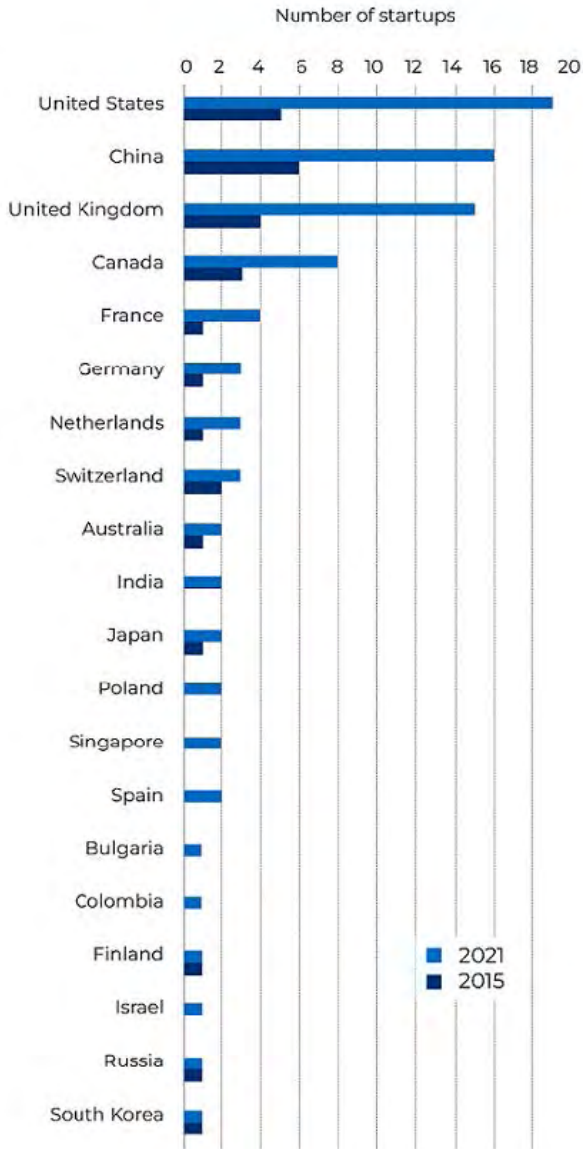
Figure 6. Private venture capital investments in quantum computing globally (World Economic Forum Report) [49]



Global venture capital investments in quantum computing have grown dramatically in recent years, across both software and hardware start-ups.

The pace of venture capital investments in quantum computing start-ups has grown dramatically in recent years (Figure 6), but this activity is largely concentrated in North America, the United Kingdom, and Europe (Figure 7). This inequity in private investment is likely to grow over the next two years as fears of global recession makes investors wary of non-established markets. Development agencies and international financial institutions like the World Bank could play central roles in filling this investment gap by becoming investors of first resort, able to attract future funding from the private sector.

Figure 7. Global distribution of quantum computing startups (World Economic Forum Report) [49]



Quantum computing start-ups are highly concentrated in high-income countries, with the vast majority found in North America, the United Kingdom, and Europe. Compared to the landscape of start-up activity in 2015, the landscape in 2021 includes some LMICs like India, Bulgaria, and Colombia, but the inequity persists as quantum computing start-up activity intensifies in high-income countries.

QUANTUM COMPUTING AND GLOBAL INEQUALITY

Quantum computing as a driver of economic inequality

Several companies, including IBM, Microsoft, Google, Amazon, and Quantinuum [58], have begun to offer time on their quantum computers via the cloud to researchers and businesses with computational problems uniquely well suited to quantum computing, such as quantum chemistry simulations. But for most applications with business value, it remains to be seen whether quantum computers will significantly outperform classical computers. Two likely scenarios for the development of the quantum technologies ecosystem can be envisioned in the near-term:

- **Quantum winter:** The current theoretical understanding of quantum computing does not guarantee quantum advantage for most computational tasks of practical interest. For some computational problems, after quantum computers were shown to outperform classical computers, parallel developments in classical computing have allowed classical computers to catch up [25,26-28]. Many academics have therefore raised concerns that the gap between promises of business-relevant applications and the limited scope of demonstrable quantum advantage represents an investment/hype bubble that will inevitably burst [59,60]. In the expected aftermath, funds and talent will be diverted in a “quantum winter,” reminiscent of similar “artificial intelligence winters” of the past.
- **Quantum spring:** Early applications, though limited and specialized, continue to attract talent and investment, until hardware improvements meet algorithmic innovations that lower stringent requirements on hardware. This yields quantum computers capable of tackling business-relevant problems. Claims of such extraordinary algorithmic advances have been met to date with widespread skepticism [33,34]. But under this scenario, quantum hardware companies will expand cloud-based quantum computing to meet growing demands from end-user businesses looking to gain an edge over competitors.

In the latter scenario, a disturbing dynamic is likely to quickly take shape: High capital costs, large lead times, and protectionism around intellectual property will likely confine quantum computers (for at least a decade) to a handful of government and corporate data centers across high-income countries. If mass proliferation via the cloud occurs concurrently, time on these quantum computers will most likely be distributed through a liberalized, market-based approach that favors those with more purchasing power. As a result, the boons of quantum computing will flow to companies and regions already at an economic advantage, underscoring existing inequalities and likely widening the global digital divide. **In short, quantum computing may engender a rich-get-richer dynamic like few technologies before.**

A quantum computer for low- and middle-income countries

The capital-intensive nature of quantum computing inspires parallels to the history of supercomputing:¹⁷ at present, the distribution of supercomputing power around the world matches levels of inequality¹⁸ seen within the most unequal domestic economies in the world [61]. If this is the scenario for supercomputing at such an advanced stage of technological maturity, the scenario for quantum computing is bleak in the absence of intervention designed to mitigate unequal access. The most concrete way to address this risk is to develop a quantum computer with cloud-based access that is either subsidized or otherwise distributed as a public good. Development of such a quantum computer is likely to require an international collaboration across several LMICs, with the involvement of research institutions in high-income countries.

There are no historical parallels for global initiatives in developing and distributing technologies that are both as capital-intensive to develop and marked by technological and economic uncertainty as quantum computers. Nonetheless, inspiration can be drawn from initiatives such as:

- **The BigScience project**, launched in 2021, has more than 1,000 researchers from 60 countries and more than 250 institutions working together to create a vast, multilingual neural network language model and multilingual text dataset on a supercomputer outside Paris, France. Designed to break the hegemony of large technology companies in AI [62], the project led to the creation of BLOOM: the largest open language model in the world built with complete transparency as a digital public good [63], capable of generation in 46 languages.
- **The Global Alliance for Vaccines and Immunization (GAVI)**, launched in 2000, brings together stakeholder organizations to address market failures in global vaccine distribution through innovative interventions like advanced market commitments [64]. GAVI has supported the immunization of 981 million children in the developing world and shipped nearly 2 billion doses of COVID-19 vaccines during the pandemic as part of the COVAX initiative [65].

Markets for allocating cloud-based quantum computing resources are likely to experience market failures for remarkably similar reasons as large language models and vaccines: prohibitive costs without price discrimination favoring high-income countries; nationalism/protectionism due to existential implications (disinformation and public health vs. national [cyber]security); and substantial commercial risk associated with uncertain demand in developing countries. However, fostering local quantum technology ecosystems can drive costs down, while funding advanced market commitments can minimize risk for private sector involvement. Examples like BigScience and GAVI suggest that any initiative to fund and coordinate the development of a subsidized/public good quantum computer for developing countries must bring together public spending, international aid, philanthropy, and innovative, market-based solutions. Countries like India, with relatively well-developed quantum strategies, could play a leading role in any such initiative, in a manner perhaps reminiscent of its significant role providing COVID-19 vaccines to the COVAX initiative.

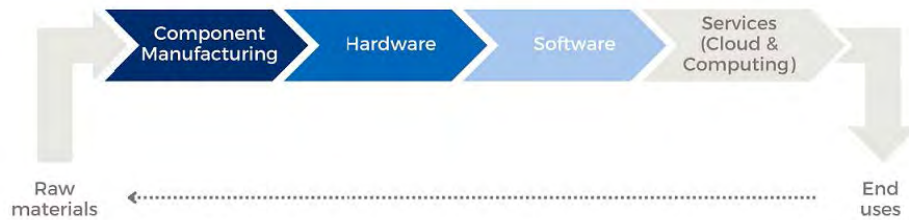
¹⁷ Supercomputers are classical computers with far more computational power than general purpose computers and are typically used in research and development and business contexts.

¹⁸ The distribution of supercomputing power has a Gini coefficient of 0.6; South Africa, the world's most economically unequal country, has a Gini coefficient of 0.63.

Supply chains and manufacturing

In the absence of home-grown quantum computing capabilities, LMICs can still secure a share of the value captured by quantum technologies by supporting local economic activity that can plug into the quantum value chain (Figure 8).

Figure 8. The quantum value chain



The quantum value chain spans economic activity ranging from raw materials that feed component manufacturing to quantum computing time distributed via the cloud for various business and research and development end uses. Notably, some end uses involving materials discovery and design optimization of components can affect both raw material markets and component manufacturing, generating a feedback loop in the quantum value chain.

Raw materials

Before settling on silicon-based transistors, classical computing went through several iterations of potential hardware architectures, with early computers based on electro-mechanical switches and on vacuum tubes. Quantum computing is at a similar point, with competing hardware architectures, each with distinct advantages and disadvantages, being developed in parallel. As a result, it is difficult to predict which hardware architecture will come to dominate the future and which critical mineral supply chains will be disrupted by the advent of quantum computing. Governments and relevant businesses should examine and explore possible futures that could be advantageous for them: for instance, if superconducting qubit-based systems employing the rare metal niobium come to dominate, countries such as Brazil that produce large quantities of niobium may stand to gain [66,67].

For the next two decades at least, the number and scale of quantum computers in the world is likely to remain small in comparison to classical computing devices.¹⁹ No major disruptions to critical mineral or other material supply chains due to quantum hardware needs are likely during that period. The sole exception may be in the production of helium, used as a cryogen to cool virtually all quantum hardware architectures. Helium is the one completely non-renewable element on earth, often lost to outer space permanently if not carefully recovered. At present, the United States dominates global helium production (with a quarter of this going to cryogenic applications)—but countries like Algeria (with sizeable helium production capacity) and Tanzania (with newfound helium deposits) stand to gain from increased quantum-related demand for cryogenics [68,69].

¹⁹ This is due to capital intensity, the limited set of computational problems with expected quantum advantage, and the exponential scaling of quantum computing power with each additional qubit, due to superposition.



Photo Credit: David Rochkind, USAID

Though we can expect limited physical proliferation of quantum computers, the biggest impact on the world's raw material supply chains may arise from their outputs. Materials discovery driven by quantum computing may yield more sustainable alternatives to the rare earth metals used in magnets and metals like lithium, nickel, and cobalt used in batteries and fuel cells [70]. The emergence of alternatives can dramatically reduce demand for associated critical mineral ores, with economic and even political ramifications for countries including:

1. Myanmar and Thailand (rare earth metals) [71]
2. Zimbabwe (lithium) [72]
3. Indonesia and the Philippines (nickel) [73]
4. Democratic Republic of Congo (cobalt) [66,74]

Component manufacturing

Critical subsystems across many quantum hardware architectures include cryogenic systems, optical components, vacuum systems, permanent magnets, and precision electronics. The low-volume, high-technology manufacturing involved in the production of these subsystems is largely dominated by China, the United States, the European Union, Japan, and Korea [75]. However, many middle-income countries in Southeast Asia (e.g., Malaysia, the Philippines, Vietnam, and Thailand) have well-developed semiconductor industries [76]. These countries can leverage the semiconductor expertise in their labor forces to diversify into niche manufacturing of components for quantum computing at costs that undercut competitors in the Global North.

Among several competing hardware realizations of quantum computers, silicon-based quantum computing, with its links to existing economic supply chains, deserves specific mention. Intel recently reported the development of silicon-based quantum devices readily fabricated by repurposing manufacturing processes used to make classical semiconductor chips [77]. Further developments may pave the way for the collective knowhow and resources of the semiconductor industry to spur rapid development of quantum computing, creating major economic opportunities for LMICs with mature semiconductor industries.

Potential applications for development

In a mature quantum computing market, i.e., with widespread proliferation via the cloud, a substantial share of the value added by quantum computing may be captured by end users, e.g., hedge funds running optimization algorithms or pharmaceuticals running simulations. According to a 2021 report by the management consulting firm Boston Consulting Group, the share of value captured by end users could be as high as 80 percent [10]. Thus, in the long-term, barring a scenario of severe quantum protectionism, LMICs may find it most fruitful to just plug into the final stage of the quantum value chain. For such countries, developing a “quantum strategy” may be as simple as forming a working group to scout and prioritize potential end uses of quantum computers. The end uses most useful to governments are likely to lie in cybersecurity and optimization in contexts from the logistics of postage to urban planning.

Quantum computing may also affect international development more broadly through its impact on critical research areas. Given this technology is still in a nascent stage, there is limited evidence about which particular applications will prove most promising long term. Still, of the Sustainable Development Goals developed by the United Nations in 2015, Zapata Computing’s former Director of Strategic Partnerships, Witold Kowalczyk, identified five that may be aided by quantum computing [78, 79]:

1. **Zero Hunger (Goal 2):** More energy-efficient methods for nitrogen fixation can be discovered with the help of quantum computers, driving food costs down and ensuring a sustainable route to zero hunger.
2. **Good Health and Well-Being (Goal 3):** Quantum simulation could substantially reduce costs and development times in drug discovery. Such improvements may play a major role in combating non-communicable diseases like cancer and heart disease and may even help to address neglected tropical diseases. Furthermore, AI trained by quantum computers may be able to identify hidden patterns across large healthcare datasets, enabling personalized, precision medicine and improved diagnostics.
3. **Clean Water and Sanitation (Goal 6):** Materials discovery through quantum simulation can accelerate the search for sustainable and cost-effective membrane technologies and catalysts for water purification.
4. **Affordable and Clean Energy (Goal 7):** Quantum optimization may play a crucial role in managing the logistics of distributed, decentralized energy networks fed by diverse renewable energy sources and handling novel energy load types like electric vehicles. Furthermore, quantum simulation is likely to play a pivotal role in the discovery of improved materials for batteries, solar panels, and wind turbines.
5. **Climate Action (Goal 13):** AI trained by quantum computers may be able to extract hidden patterns from large amounts of meteorological data, allowing improved projections for global climate change and even predictions of extreme weather events.

It is difficult to say with certainty if (and when) any of these applications will materialize, as we have not yet conclusively demonstrated quantum advantage for truly societally relevant problems.

RECOMMENDATIONS: MANAGING RISKS AND OPPORTUNITIES OF QUANTUM FOR GLOBAL DEVELOPMENT

Progress in quantum computing, like that of many other emerging technologies, continues to be driven largely by the private sector. Public sector initiatives to accelerate innovation in quantum information are relatively recent and concentrated primarily in developed countries. In the United States, for example, the National Quantum Initiative Act of 2018 called for a 10-year plan and for US\$1.25 billion in funding over the first five years from the Department of Energy to support research, foster development of a quantum technology ecosystem, and encourage industry participation. US\$877 million was allocated to the program in 2022.

Resource constraints, both in investment capital and human capital, make LMICs especially vulnerable to the risks posed by a quantum computing future. First among these are the cybersecurity risks of quantum computers able to break public-key cryptography currently used on digital systems. LMICs must also invest in a workforce that can benefit from economic tailwinds from the deployment of quantum computers at scale. Finally, there may be undiscovered opportunities for leapfrogging economic progress in LMICs through research and development and supply-chain innovations that can be realized only through proactive cross-sector collaboration between researchers in academia and industry practitioners.

USAID is uniquely positioned to make investments that can help LMICs manage risks from the quantum computing transition and benefit from the economic growth it will enable. Quantum computing will have profound implications for many core sectors that are priorities for USAID and other development agencies: digital inclusion, cybersecurity, and workforce development. While development practitioners may not be experts in quantum computing, they must consider the risks and opportunities this new technology presents, learning through dialogue with researchers and industry experts. Keeping this in mind, we break down our recommendations for managing the risks and opportunities of quantum computing for global development into three pillars:

- **Preparing for cybersecurity risks from quantum computing:** In the most immediate future, USAID should endeavor to help LMICs make their digital systems “quantum-ready.” This would ensure that existing digital platforms, especially in banking, health care, and communications (e.g., secure messaging services or end-to-end encrypted messaging platforms like WhatsApp), are resilient to cybersecurity risks due to quantum computing.
- **Investing in quantum computing–ready human capital:** Existing higher educational institutions in LMICs lack the capacity to develop a quantum computing ready workforce. USAID should partner with university systems and support ministries of education to develop that human capital.
- **Building research and development ecosystems:** Research and development investments in emerging technologies are significantly lower in LMICs compared to such investments in developed countries. USAID can support building new institutions dedicated to quantum computing and incentivize collaborations between researchers from developing countries and the United States. As quantum technologies mature, the demand for quantum hardware can boost manufacturing in specific LMICs. Such countries can leverage existing supply chains to benefit from this demand. USAID can help with early-scoping and building investment theses for supply chains beneficial to the economy of the United States and that allow partner countries to reap economic benefits from quantum technologies.

With quantum technology still in the early stages of maturation, we caution against unwarranted conservatism or optimism. Failing to recognize the potential of quantum technologies early can have serious opportunity costs for LMICs. On the other hand, investing resources in areas where the impact of quantum technologies remains uncertain can lead to poor allocation of resources. Keeping this in mind, we highlight which recommendations will be most beneficial regardless of the timeline and direction that quantum computing takes, and which may be more contingent.

Equipping LMICs for cybersecurity risks from quantum computing

The most urgent near-term threat for LMICs from quantum technologies is the development of cryptographically capable quantum computers. Such computers would be capable of breaking the public-key cryptography used on most digital systems around the world. Their proliferation could potentially jeopardize critical infrastructure underlying financial services, civilian communications, and national security. This imminent risk has been recognized by the highest levels of the United States government, as reflected in the national security memorandum on quantum computing signed by President Joe Biden on May 4, 2022 [80].

USAID can play a crucial role in helping developing country governments and NGOs transition existing standards for public-key cryptography to quantum computing-resistant cryptographic systems. Quantum computing-resistant cryptography protocols already exist. However, a timely transition to those protocols requires technical capabilities that LMIC governments often lack.

Additionally, LMIC governments should be aware that data recorded with current encryption standards can later be decrypted by operators of a future cryptographically relevant quantum computer. This implies institutions cannot merely shift to new encryption protocols for data collected in the future; current sensitive data needs to be encrypted in a quantum-resistant manner. This is likely to require significant capital investments. USAID can play a central enabling role in this transition.

A short-term, high-impact strategy for USAID to assist LMICs is to establish a “Global Quantum Transition Taskforce” that will aid LMIC governments and private sector NGO partners in transitioning to quantum-safe cryptography in widely used digital systems. This task force can provide guidelines and technical support to developing countries to bridge technical talent gaps discussed earlier. It can also provide pooled capital to LMIC governments to transition existing data to quantum-safe encryption.

Investing in quantum-ready human capital

As public and private funding for quantum computing booms, a key bottleneck identified by industry watchers is the lack of quantum-ready talent to take advantage of this growth in funding. The demographic dividend in many LMICs can be leveraged to fill this talent gap in quantum computing. However, the current curricula and the quality of higher education institutions pose a challenge in developing quantum-ready talent in developing countries.

To ensure the future workforce can benefit from the quantum revolution, USAID can assist governments and universities in LMICs to create new talent pipelines for the quantum industry. We recommend USAID take a two-pronged approach. First, support universities and startups in developing countries in building new curricula for quantum talent by launching new degree programs and bootcamps. Second, work with governments and higher education institutions to generate awareness around the quantum computing transition and opportunities that can attract top talent to take these courses.

Importantly, experts we spoke to emphasized the need for cross-disciplinary talent with both technical skills in quantum computing as well as broad industry insights developed through business degrees (i.e., Master of Business Administration).

Building research and development ecosystems

As discussed in Section 5, there is a massive investment gap in quantum research and development between LMICs and developed countries (the United States, the United Kingdom, the European Union, and China). While it is not feasible for USAID alone to fill this investment gap, it can support the creation of a global quantum research and development ecosystem that can attract future investment from both the private sector and developing country governments.

USAID can invest in building such ecosystems by enabling research collaborations between quantum researchers in LMICs and universities in the United States. Opportunities for developing country researchers to spend up to a year in a host United States university can enable creation of new research partnerships. USAID can support existing programs like the Quad Fellowship, which aims to support graduate students from the Quad countries (including India) to obtain advanced degrees in quantum computing at universities in the United States. USAID could support the development of new departments of quantum computing at universities in developing countries. Finally, we recommend USAID support an annual “Quantum Computing for Development” conference—or create such a track at an existing technology and international development conference—to encourage collaborations between researchers, industry experts, and policymakers.

Developing countries may not be able to proactively leverage existing supply chains to benefit from the manufacturing boom that would accompany a quantum transition. For instance, cooling systems are a critical part of quantum computers, and some LMICs may already possess a competitive advantage in manufacturing these systems at low-cost. USAID could facilitate high-level dialogue between quantum computing experts, industry leaders, and chambers of commerce in developing countries to identify opportunities for existing industries to benefit from manufacturing demand that accompanies the quantum transition.

REFERENCES

- [1] Samantha Brookman. "15 Huge Supercomputers That Were Less Powerful Than Your Smartphone." The Clever, April 18, 2017. <https://www.theclever.com/15-huge-supercomputers-that-were-less-powerful-than-your-smartphone/>.
- [2] Hugh J. Watson. "Tutorial: Big data analytics: Concepts, technologies, and applications." Communications of the Association for Information Systems 34, (2014): 65. <https://doi.org/10.17705/ICAIS.03462>.
- [3] Jonathan P. Dowling, and Milburn, Gerard J. "Quantum technology: the second quantum revolution." Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences 361, no. 1809 (2003): 1655-1674. <https://doi.org/10.1098/rsta.2003.1227>.
- [4] European Quantum Flagship. Strategic Research Agenda, 2020. https://qt.eu/app/uploads/2020/04/Strategic_Research_Agenda_d_FINAL.pdf.
- [5] Niko Mohr, Masiowski, Mateusz, Zesko, Matija, and Soller, Henning. "Quantum Technology Monitor." McKinsey & Company, June 2022. <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20funding%20remains%20strong%20but%20talent%20gap%20raises%20concern/quantum-technology-monitor.pdf>.
- [6] A. K. Fedorov, Gisin, N., Belousov, S. M., and Lvovsky, A. I. "Quantum computing at the quantum advantage threshold: a down-to-business review." arXiv 2203, no. 17181 (March 31, 2022). <https://arxiv.org/pdf/2203.17181.pdf>.
- [7] Gaurav Batra, Gschwendtner, Martina, Ostojic, Ivan, Queirolo, Andrea, Soller, Henning and Wester, Linde. "Shaping the long race in quantum communication and quantum sensing." McKinsey & Company, December 21, 2021. <https://www.mckinsey.com/industries/advanced-electronics/our-insights/shaping-the-long-race-in-quantum-communication-and-quantum-sensing>.
- [8] Roger A. Grimes. Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto. Hoboken: John Wiley & Sons, 2020.
- [9] Matteo Biondi, Heid, Anna, Ostojic, Ivan, Henke, Nicolaus, Pautasso, Lorenzo, Mohr, Niko, Wester, Linde and Zimmel, Rodney. "Quantum computing: An emerging ecosystem and industry use cases." McKinsey & Company, December 2021. <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20use%20cases%20are%20getting%20real%20what%20you%20need%20to%20know/quantum-computing-an-emerging-ecosystem.pdf>.
- [10] Jean-François Bobier, Langione, Matt, Tao, Edward and Gourevitch, Antoine. "What Happens When 'If' Turns to 'When' in Quantum Computing?" Boston Consulting Group, July 2021. <https://web-assets.bcg.com/89/00/d2d074424a6ca820b1238e24ccc0/bcg-what-happens-when-if-turns-to-when-in-quantum-computing-jul-2021-r.pdf>.

- [11] Lennart Baumgärtner, Klein, Benjamin, Mohr, Niko, Pflanzner, Anika & Soller, Henning. “When—and how—to prepare for post-quantum cryptography.” McKinsey & Company, May 4, 2022. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography>.
- [12] National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. edited by Emily Grumbling and Horowitz, Mark. Washington DC: The National Academies Press, 2019. <https://doi.org/10.17226/25196>.
- [13] Richard P. Feynman. “Simulating physics with computers.” International Journal of Theoretical Physics 21, (1982): 467-488. <https://doi.org/10.1007/BF02650179>.
- [14] John Preskill. “Quantum computing 40 years later.” arXiv 2106, no. 10522. (June 6, 2021): <https://arxiv.org/pdf/2106.10522.pdf>.
- [15] Alexandre Ménard, Ostojic, Ivan, Patel, Mark and Volz, Daniel. “A gameplan for quantum computing.” McKinsey Quarterly, February 6, 2020. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing>.
- [16] Matthias Evers, Heid, Anna and Ostojic, Ivan. “Pharma’s digital Rx: Quantum computing in drug research and development.” McKinsey & Company, June 18, 2021. <https://www.mckinsey.com/industries/life-sciences/our-insights/pharmas-digital-rx-quantum-computing-in-drug-research-and-development>.
- [17] Ondrej Burkacky, Mohr, Niko, and Pautasso, Lorenzo. “Will quantum computing drive the automotive future?” McKinsey & Company, September 2, 2020. <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/will-quantum-computing-drive-the-automotive-future>.
- [18] Elena Yndurain and Kesterson-Townes, Lynn. “Prioritizing quantum computing applications for business advantage: charting a path to quantum readiness.” IBM Institute for Business Value, Research Insights, June 2020. <https://www.ibm.com/downloads/cas/JRKDYED0>.
- [19] Hannah Fry. Hello World: How to be Human in the Age of the Machine. London: Transworld Publishers, 2018.
- [20] Payal Dhar. “The carbon impact of artificial intelligence.” Nature Machine Intelligence 2, no. 8 (2020): 423-425. <https://doi.org/10.1038/s42256-020-0219-9>.
- [21] Roy Schwartz, Dodge, Jesse, Smith, Noah A., and Etzioni, Oren. (2020). “Green AI.” Communications of the ACM 63, no. 12 (December 2020): 54-63. <https://doi.org/10.1145/3381831>.
- [22] Jacob Biamonte, Wittek, Peter, Pancotti, Nicola, Rebentrost, Patrick, Wiebe, Nathan, and Lloyd, Seth. (2017). “Quantum machine learning.” Nature 549, no. 7671 (2017): 195-202. <https://doi.org/10.1038/nature23474>.

- [23] Jens Backes, Dietz, Miklos, Henke, Nicolaus, Moon, Jared, Pautasso, Lorenzo, and Sadeque, Zaheen. "How quantum computing could change financial services." McKinsey & Company, December 18, 2020. <https://www.mckinsey.com/industries/financial-services/our-insights/how-quantum-computing-could-change-financial-services>.
- [24] Peter Cooper, Ernst, Philipp, Kiewell, Dieter and Pinner, Dickon. "Quantum computing just might save the planet." McKinsey & Company. May 19, 2022. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/quantum-computing-just-might-save-the-planet>.
- [25] Jun-Ting Hsieh. "Quantum Complexity Theory." TCS Toolkit Writing Project, 2020. <https://jthsieh.github.io/files/projects/BQP.pdf>
- [26] Ewin Tang. "A quantum-inspired classical algorithm for recommendation systems." Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, (June 2019): 217-228. <https://doi.org/10.1145/3313276.3316310>.
- [27] Yong Liu, Liu, Xin, Li, Fang, Fu, Haohuan, Yang, Yuling, Song, Jiawei, Zhao, Pengpeng, et al. "Closing the 'quantum supremacy' gap: achieving real-time simulation of a random quantum circuit using a new sunway supercomputer." In Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis, (November 2021): 1-12. <https://doi.org/10.1145/3458817.3487399>.
- [28] Hsin-Yuan Huang, Kueng, Richard, Torlai, Giacomo, Albert, Victor V., and Preskill, John. "Provably efficient machine learning for quantum many-body problems." Science 377, no. 6613 (2022): <https://doi.org/10.1126/science.abk3333>.
- [29] "Quantum cryptography in real-world applications." QuantLR. 2023. <https://quantlr.com/quantum/quantum-cryptography-in-real-world-applications/>.
- [30] C. L. Degen, Reinhard, F., and Cappellaro, P. "Quantum Sensing." Reviews of Modern Physics 89, no. 3 (July 2017): 035002. <https://doi.org/10.1103/RevModPhys.89.035002>.
- [31] UK National Quantum Technologies Programme. A roadmap for quantum technologies in the UK, 2015. <https://uknqt.ukri.org/wp-content/uploads/2021/10/National-Quantum-Technologies-Roadmap.pdf>.
- [32] Hugh Collins and Nay, Chris, "IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two." International Business Machines Corporation 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>.
- [33] Bao Yan, Tan, Ziqi, Wei, Shijie, Jiang, Haocong, Weilong, Wang, Wang, Hong, Luo, Lan, et al. "Factoring integers with sublinear resources on a superconducting quantum processor." arXiv 2212, no. 12372 (2022): <https://arxiv.org/pdf/2212.12372.pdf>.
- [34] Scott Aaronson. "Cargo Cult Quantum Factoring." Shtetl-Optimized, January 4, 2023. <https://scottaaronson.blog/?p=6957>.

- [35] Johnny Kung, and Fancy, Muriam. "A Quantum Revolution: Report on global policies for quantum technology." Canadian Institute for Advanced Research, April 2021. <https://cifar.ca/wp-content/uploads/2021/04/quantum-report-EN-10-accessible.pdf>.
- [36] Michele, Mosca and Piani, Marco. "2021 quantum threat timeline report." Global Risk Institute, January 24, 2022. <https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/>.
- [37] Jaime Sevilla and Riedel, C. Jess. "Forecasting timelines of quantum computing." arXiv 2009, no. 05045. (December 9, 2020): <https://arxiv.org/pdf/2009.05045.pdf>.
- [38] Scott Aaronson. Quantum computing since Democritus. Cambridge: Cambridge University Press, 2013.
- [39] "The Leading Edge of Quantum Computational Chemistry." Quantinuum, 2022. <https://www.quantinuum.com/computationalchemistry/inquanto>.
- [40] National Institute of Standards & Technology, Computer Security Resource Center. Post-Quantum Cryptography, January 3, 2017. <https://csrc.nist.gov/projects/post-quantum-cryptography>.
- [41] John P. Mello Jr., "NIST Action Will Heat Up Post-Quantum Cryptography Market: Report." Tech News World, December 9, 2022. <https://www.technewsworld.com/story/nist-action-will-heat-up-post-quantum-cryptography-market-report-177493.html>.
- [42] NSA Media Relations. "NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems." National Security Agency, November 9, 2022. <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/>.
- [43] "Open Quantum Safe: software for prototyping quantum-resistant cryptography." The Open Quantum Safe Project, 2017. <https://openquantumsafe.org/>.
- [44] Rebecca Winthrop, Barton, Adam, and McGivney, Eileen. Leapfrogging Inequality: Remaking Education to Help Young People Thrive. Washington, DC: Brookings Institution Press, 2018.
- [45] The World Bank, UNESCO and UNICEF. The State of the Global Education Crisis: A Path to Recovery. Washington D.C., Paris, New York: The World Bank, UNESCO, and UNICEF, 2021.
- [46] Mateusz Masiowski, Mohr, Niko, Soller, Henning and Zesk, Matija. "Quantum computing funding remains strong, but talent gap raises concern." McKinsey & Company, June 15, 2022. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern>
- [47] Subcommittee on Quantum Information Science, Committee on Science of the National Science & Technology Council. "Quantum Information Science and Technology Workforce Development National Strategic Plan." Executive Office of the President of the United States, February 2022. <https://www.quantum.gov/wp-content/uploads/2022/02/QIST-Natl-Workforce-Plan.pdf>.

- [48] Laurent Belsie. "Immigrants play a key role in STEM fields," National Bureau of Economic Research: The Digest, no. 11 (November 2016). <https://www.nber.org/digest/nov16/immigrants-play-key-role-stem-fields>.
- [49] Jerry Chow, Greplová, Eliška, Heijman, Freeke, Kuchkovsky, Carlos, O'Halloran, Derek, Pointing, Jessica, Shutko, Grigory, and Williams, Carl J. "State of quantum Computing: Building a quantum economy." World Economic Forum Insight Report, September 2022. https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf.
- [50] Elias G. Carayannis, Draper, John, and Bhaneja, Balwant. "Towards fusion energy in the Industry 5.0 and Society 5.0 context: Call for a global commission for urgent action on fusion energy." Journal of the Knowledge Economy 12, no. 4 (2021): 1891-1904. <https://doi.org/10.1007/s13132-020-00695-5>.
- [51] Daniel Bashir. "GPT-3, Foundation Models, and AI Nationalism: Geopolitical Implications of the 'Year of Monster Models.'" Last Week in AI, December 30, 2021. <https://lastweekin.ai/p/gpt-3-foundation-models-and-ai-nationalism>.
- [52] Peter Elstrom, Gao, Yuan and Liu, Coco. "China's 'little giants' are its latest weapon in the U.S. tech war." Bloomberg Europe Edition, January 2022. <https://www.bloomberg.com/news/articles/2022-01-23/china-us-xi-jinping-backs-new-generation-of-startups-in-tech-war>.
- [53] Scarlett Evans. "What the CHIPS Act means for quantum computing." Enter Quantum, August 10, 2022. <https://www.quantumbusinessnews.com/deals-partnerships/what-the-chips-act-means-for-quantum-computing>.
- [54] Mateo Aboy, Minssen, Timo and Kop, Mauritz. "Mapping the patent landscape of quantum technologies: Patenting trends, innovation and policy implications." IIC - International Review of Intellectual Property and Competition Law 53, (May 2022): 853-882. <https://doi.org/10.1007/s40319-022-01209-3>.
- [55] Achyuta Ghosh and Khanna, Akshay. "The Quantum Revolution in India: Betting Big on Quantum Supremacy." Nasscom & Avasant, February 2022. <https://avasant.com/report/the-quantum-revolution-in-india-betting-big-on-quantum-supremacy/>.
- [56] "Quad Joint Leaders' Statement." The White House Briefing Room Statements and Releases, May 24, 2022. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/>.
- [57] "FACT SHEET: United States and India Elevate Strategic Partnership with the initiative on Critical and Emerging Technology (iCET)" The White House Briefing Room Statements and Releases, January 31, 2023. <https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/31/fact-sheet-united-states-and-india-elevate-strategic-partnership-with-the-initiative-on-critical-and-emerging-technology-icet/>.
- [58] James Dargan. "13 Companies Offering Quantum Cloud Computing Software Services." The Quantum Insider, May 3, 2022. <https://thequantuminsider.com/2022/05/03/13-companies-offering-quantum-cloud-computing-services-in-2022/>.

- [59] John Horgan. "Will Quantum Computing Ever Live Up to Its Hype?" Scientific American, April 20, 2021. <https://www.scientificamerican.com/article/will-quantum-computing-ever-live-up-to-its-hype/>.
- [60] Sankar Das Sarma. "Quantum computing has a hype problem." MIT Technology Review, March 28, 2022. <https://www.technologyreview.com/2022/03/28/1048355/quantum-computing-has-a-hype-problem/>.
- [61] Joab Jackson. "Top500 shows growing inequality in supercomputing power." ComputerWorld, November 13, 2013. <https://www.computerworld.com/article/2486186/top500-shows-growing-inequality-in-supercomputing-power.html>.
- [62] BigScience. "A one-year long research workshop on large multilingual models and datasets." Hugging Face, 2022. <https://bigscience.huggingface.co/>.
- [63] "Digital Public Goods." Digital Public Goods Alliance, 2023. <https://digitalpublicgoods.net/digital-public-goods/>.
- [64] Owen Barder, Kremer, Michael, and Levine, Ruth. "Making markets for vaccines: Ideas to action." Report of the Center for Global Development, 2005. <https://www.med.upenn.edu/istar/PDF-literature-photos/MakingMarkets-complete.pdf>.
- [65] Gavi, the Vaccine Alliance, 2022. <https://www.gavi.org/>.
- [66] Robert M. Callaghan. "Niobium (Columbium)." United States Geological Survey, Mineral Commodity Summaries, January 2021. <https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-niobium.pdf>.
- [67] P. Emsbo, Lawley, C., and Czarnota, K. "Geological surveys unite to improve critical mineral security." Eos, February 5, 2021. <https://eos.org/science-updates/geological-surveys-unite-to-improve-critical-mineral-security>.
- [68] Joseph B. Peterson. "Helium." United States Geological Survey, Mineral Commodity Summaries, January 2022. <https://pubs.usgs.gov/periodicals/mcs2022/mcs2022-helium.pdf>.
- [69] Matt Reynolds. "Huge underground helium reserve discovered in Tanzania." Wired, June 30, 2016. <https://www.wired.co.uk/article/huge-helium-reserve-discovered-in-tanzania>.
- [70] Christoph Steitz and Waldersee, Victoria. "Bosch, IBM join forces to seek substitute critical minerals." Reuters, November 9, 2022. <https://www.reuters.com/technology/germanys-bosch-partners-with-ibm-quantum-computing-2022-11-09/>.
- [71] Daniel J. Cordier. "Rare Earths." United States Geological Survey, Mineral Commodity Summaries, January 2022. <https://pubs.usgs.gov/periodicals/mcs2022/mcs2022-rare-earth.pdf>.
- [72] Brian W. Jaskula. "Lithium." United States Geological Survey, Mineral Commodity Summaries, January 2022. <https://pubs.usgs.gov/periodicals/mcs2022/mcs2022-lithium.pdf>.

- [73] Michele E. McRae. "Nickel." United States Geological Survey, Mineral Commodity Summaries, January 2022. <https://pubs.usgs.gov/periodicals/mcs2022/mcs2022-nickel.pdf>.
- [74] Kim B. Shedd. "Cobalt." United States Geological Survey, Mineral Commodity Summaries, January 2022. <https://pubs.usgs.gov/periodicals/mcs2022/mcs2022-cobalt.pdf>.
- [75] "Proportion of Total Manufacturing Value Added from Medium and High-tech Industry." Our World in Data, 2019. <https://ourworldindata.org/grapher/total-manufacturing-value-added-from-high-tech>.
- [76] Datawheel and Centre for Collective Learning. "Integrated Circuits." The Observatory of Economic Complexity, 2020. <https://oec.world/en/profile/hs/integrated-circuits>.
- [77] Intel Public Relations. "Intel hits key milestone in quantum chip production research." Intel Corporation, October 5, 2022. <https://www.intel.com/content/www/us/en/newsroom/news/intel-hits-key-milestone-quantum-chip-research.html#gs.f0oyzl>.
- [78] Witold W. Kowalczyk. "Let's make quantum computing about sustainability." Zapata Computing, January 22, 2020. <https://www.zapatacomputing.com/lets-make-quantum-computing-about-sustainability/>.
- [79] Erika Karp, Peters, Mark, Workman, John, Erondy, Jude, Hsueh, Eric, Yang, Heng, Jabusch, Garvin, et al. "Quantum Impact" – The Potential for Quantum Computing to Transform Everything." Pathstone, The Modern Family Office, December 10, 2021. <https://www.pathstone.com/quantum-impact-the-potential-for-quantum-computing-to-transform-everything/>.
- [80] "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." The White House Briefing Room Statements and Releases, May 04, 2022. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>.

Get involved!

If you are interested in learning more about quantum computing for development, please contact: digitaldevelopment@usaid.gov





USAID
FROM THE AMERICAN PEOPLE