Vol. 47, January 2024

MITCHELL INSTITUTE
Policy Paper

The Quantum Advantage: Why it Matters and Essential Next Steps

Part 2: The Promise of Quantum Computing

by Heather R. Penney
Senior Resident Fellow, The Mitchell Institute for Aerospace Studies

Key Points

Quantum science has advanced to the point where technologists can directly control, manipulate, and measure particles at the subatomic level. This has profound implications for quantum information science and technology, including the field of computing.

Quantum bits, or "qubits," are the basic information units in quantum computing. Analogous to bits in today's binary computers, qubits are subatomic particles that store information. Subatomic quantum behaviors and attributes such as particle superposition, entanglement, and interference enable quantum computers to compute algorithms that are considered "intractable," or impossible, for today's most advanced binary computers.

Quantum computers are not just "super-fast supercomputers." Quantum computers are best considered extremely powerful machines that can specialize in solving specific problem sets like combinatoric or factorization calculations, optimization problems, machine learning, and molecular modeling.

Qubits are extremely sensitive and, therefore, vulnerable to external stimuli and signals that induce errors. And since different qubit modalities and designs will have different error rates, it is not possible to measure the power of a quantum computer simply by counting its absolute number of qubits.

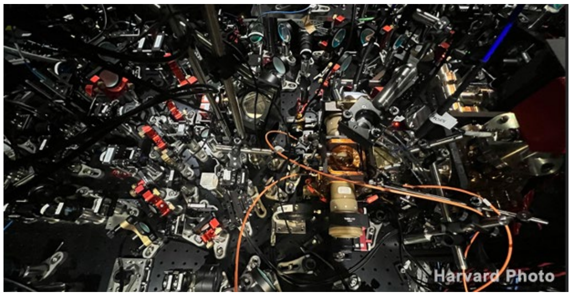
Scientists are working to develop "benchmarking" methodologies to measure and compare the power and progress of quantum computers for pragmatic operations. Developing useful quantum computers that can solve real-world problems will require a dedicated national-level effort.

Abstract

This report is the second of a three-part series intended to educate senior U.S. defense leaders about quantum technologies. The first report provides a basic explanation of the quantum science that underpins this rapidly developing field. The final report provides U.S. defense policymakers with an overview of the quantum defense industrial base. This, the second report of the series, builds on core principles of quantum science explained in the first report to present an overview of quantum computers, their critical components, how they work, and their potential applications.

The ability to directly control, manipulate, and measure subatomic particles to exploit the unique properties of quantum mechanics has the potential to revolutionize computer processing. The impact of quantum computing promises to rival or even exceed that of the development of semiconductors on modern computation.

Given the transformative potential of quantum computing—and the hype that often surrounds it—U.S. defense policymakers should have a working understanding of quantum computers, their critical components, how they function, and applications they may be able to perform. A basic understanding of these fundamentals is an essential step toward evaluating progress in quantum technology development and the potential for different quantum computing approaches to meet future operational requirements.



DARPA's Optimization with Noisy Intermediate-Scale Quantum devices (ONISQ) program funds this picutred Harvard experiment "featuring optical paths for a novel, reconfigurable quantum computing architecture."

Credit: Harvard University/DARPA

Introduction

In the 1980s, the transition from vacuum tubes to solid-state transistors made the revolution in military affairs possible because semiconducting chips made computers faster, more efficient, more reliable, and far more compact. This advanced processing is now the foundation of nearly every modern military capability, including datalinks, battle management networks, data fusion technologies, and other advanced systems that have moved warfare from the industrial age to the information era.[1] Quantum computers hold a similar potential to revolutionize warfare.[2]

Quantum computers are best understood as extremely powerful, specialized processors that will have the ability to solve problems that today's fastest supercomputers cannot. Applications will include cracking the most advanced encryption schemes, modeling complex chemical and biological interactions, solving thorny optimization problems, and rapidly advancing machine learning. The fields that quantum computers will impact span everything from financial markets to national security, intelligence, and logistics. The full consequences of quantum computing have yet to be imagined, but one thing is clear: the nation that develops a pragmatic quantum computing capability will wield an important advantage over its competitors.

The nation that develops a pragmatic quantum computing capability will wield an important advantage over its competitors.

American industry is vigorously pursuing quantum computing and currently holds the lead in its development. This does *not* mean that U.S. policymakers should assume this lead will continue. China understands the significance of achieving a quantum advantage and is aggressively pursuing a practical quantum computer. In 2021, the University of Science and Technology of China (USTC) revealed an advanced superconducting computer, the Zuchongzhi, which worked out a problem three times tougher than Google's 53-qubit Sycamore computer could solve.[3] That same year, they also demonstrated Jiuzhang 2, a 113-photonic qubit computer whose computational speed and power exceeded the Google Sycamore computer.[4] Chinese academia, which is inextricably linked with China's People's Liberation Army (PLA), is clearly vying to establish its leadership position in the field of quantum computing.

The Biden administration recognizes that "America's continued technological and scientific leadership will depend, at least in part, on the Nation's ability to maintain a competitive advantage in quantum computing and QIS [quantum information science]."[5] To best support and resource the development and fielding of pragmatic and superior quantum computers, senior U.S. national security leaders and policymakers must have a deeper technical understanding of these machines. This paper provides a basic overview of what quantum computers are, their critical components, how they work, what they can do, and how to evaluate progress in this field.

Quantum Computers Can Solve Problems That Are Impossible for Binary Computers

Intractable problems for which quantum computers excel

Contrary to popular perception, quantum computers are not super-fast supercomputers. In fact, there are many computational tasks and software programs that quantum engineers consider modern binary computers faster, more efficient, and far more accurate tools.[6] However, quantum computers hold exceptional promise when it comes to important problems that the world's best binary computers *cannot* solve.[7] While the full range of applications for quantum computers is not yet defined, experts anticipate that the unique properties of qubits and quantum algorithms will be well-suited for material sciences and molecular-level modeling, accelerating the development of machine learning technologies critical to artificial intelligence, solving complex optimization problems, and other defense and non-defense applications.[8]

- **Material sciences and properties.** Quantum computers will have the ability to model and simulate the properties of complex molecular structures, opening the way to develop exotic or unknown materials that apply to aerospace capabilities, such as advanced stealth coatings, hypersonic materials, or sensor bodies.[9]
- **Machine learning.** Quantum algorithms and computation have the potential to improve machine learning algorithms with significantly fewer training data requirements. Practical military applications for quantum machine learning could include the development of new algorithms to improve target recognition and identification, electronic warfare applications to counter a threat, or enhanced capabilities for battlespace situational awareness when an adversary presents novel signatures in the electromagnetic spectrum.[10]
- **Complex optimization problems.** These types of problems tackle complex systems or interactions with many different variables to find the best solution based on prioritized factors. Military applications might include planning logistic sorties and loads for agile combat employment (ACE) bases, real-time aerial refueling tanker positioning and offloads, real-time advanced battle management target pairing, unmanned aerial vehicle (UAV) swarm management, or other mission planning tasks.
- **Decryption of factorization-based data and communications.** Modern encryption is often based on factorization, which requires solving for the two unique multipliers (or factors) of a large number. Breaking factorization-based encryption is a challenge that exceeds the ability of today's most advanced binary computers. Quantum computers will be able to quickly solve large number factorization problems using Shor's algorithm. While nascent "quantum-resistant" encryption is in use today, militaries could collect and store factorization-based encrypted data with the intent of decrypting it in the future using quantum computing technologies.[11]
- **Chemical reactions.** The ability of quantum simulators and computers to model the highly complex dynamics of chemical reactions may be crucial to developing next-generation energetics for propulsion and other capabilities that can create kinetic effects.[12] These technologies could be particularly useful for U.S. military and civilian space entities as they compete with China to establish and maintain a presence in the vast cislunar regime that lies between the Earth and the moon.[13]

It is important to note that while the above use cases are potential opportunities based on what is now known about quantum mechanics, they are still mostly speculative. Quantum computers have not yet matured sufficiently to demonstrate conclusively their advantage over classical binary computers in these applications. This said the most advanced classical computers are not good at these problems either, and adversaries are aggressively developing quantum computing technologies to gain an advantage that will translate to real battlefield effects. U.S. policymakers should be mindful that the opportunity cost of *not* pursuing quantum computation may be much higher than doing so, even if early technological aimpoints do not pan out. The potential for uses and applications that have not yet been considered is just as important to account for, as further discovery requires time and resources upfront for the development of first-generation quantum devices.

U.S. policymakers should be mindful that the opportunity cost of *not* pursuing quantum computation may be much higher than doing so.

Understanding the "Magic" of Quantum

Qubits encode information differently than classical, binary bits

A quantum bit, or qubit, is simply the most basic unit of quantum information. A classical bit in traditional computing is binary in nature: it is either in a 1 or 0 state. These states are related to how the bit is physically built. In early computers, bits were electrical transistors that were either powered on (a state of 1) or powered off (a state of 0).[14] The difference between a bit and a qubit is that a qubit can also be in a state of **superposition**, a combination state between 1 and 0. At the physical level, qubits can be made from different types of particles: electrons, ions, atoms, or photons. The informational value of the qubit is represented by physical attributes like spin up or spin down, spin clockwise or anti-clockwise, or the vertical or horizontal polarization of the particle.[15] In practical terms, this means a qubit can be in multiple states at the same time. This means they have the potential to represent far more states, or data, than a binary 1 or 0 bit.

Importantly, the state or value of the qubit is not known until it is measured. It is neither 1 nor 0—in a superposition state, it is both 1 *and* 0. This unique state or value can also be understood as a simultaneous probability that, when measured or observed, "collapses" into *either* 1 *or* 0. The value of a qubit and the outcome of a larger quantum system is manipulated through properties called interference and entanglement.

Interference can be used to manipulate & change quantum systems

Subatomic matter interacts in a dynamic called **interference.**[16] Interference is the means to manipulate qubits to perform algorithms and other complex logic functions. Unlike classical representations where atoms bounce off each other like billiard balls on a pool table, interference is best visualized as ripples on a pond, waves in the ocean, or even soundwaves in noise-canceling headsets where the wave properties of matter interact with each other to amplify, null, or otherwise alter the wave pattern.[17] Scientists have long established that subatomic particles behave like waves—a principle called **wave-particle duality**—and they represent quantum matter mathematically as a **wavefunction**. Interference between wavefunctions unites their characteristics and can change the amplitude, frequency, or other properties of the combined wavefunction.[18]

Entanglement scales how qubits compute

Interference can also be used to entangle particles. **Entanglement** is a phenomenon where quantum particles are generated, interact, or share an external stimulus in a way that creates a perfect correlation between them.[19] This does not necessarily mean that entangled particles are identical. Instead, entangled particles behave as a single, integrated system—a common, unified quantum state where the properties of any one particle are dependent on the properties of other particles.[20] In other words, entanglement causes particles to lose their individuality and *act as a coherent entity or system*.[21] Thus, interfering or stimulating one qubit will affect all other qubits with which it is entangled.[22]

Superposition, interference, & entanglement are the key to quantum's computational power

Classical computers are binary—they can only be in one state at any point in time and thus are linear in the way they perform computations. This means multiple input variables, complex algorithms, and the number of steps required to solve certain problems can exceed the computer's available computational capacity or require an exponential amount of time.[23] Computer scientists describe these kinds of challenging calculations as intractable. Quantum computers will excel at solving these kinds of intractable problems because they can harness the unique quantum properties of superposition, entanglement, and interference to calculate using non-binary and multi-dimensional states.

Consider the computational volume of classical bits versus qubits. Binary and linear classical computers have bits in a singular state of either 0 or 1. Because the bits are independent from each other and are connected only through their gate logic, their computational power is simply additive: each bit can only contribute one additional piece of computation.[24]

The potential computational power of quantum devices, however, is exponential because of superposition: quantum computers can be in many different states between 1 and 0 at the same time. A qubit remains in superposition until it is observed or measured, at which point it collapses into a traditional, binary state. When qubits are entangled, their computational power will be the result of the probability distribution of each entangled qubit in the system. Thus, a two-qubit entangled system has four potential values; a three-qubit entangled system has eight potential values; a four-qubit entangled system has a probability distribution of sixteen states; and so on. A quantum computer can be in 2 to the power of "n" states, which means scaling qubits has an exponential impact on total computational power.[25]

Correcting for the sensitivity of qubits

A major challenge for any quantum system, regardless of the method used to create and control its qubits—or its **modality**[26]—is that the inherent sensitivity and fragility of qubits makes them prone to error, or wrong answers. The same quantum principles that make qubits so useful for computation also make them vulnerable to "noise."[27] Noise from the environment—such as radiation, heat, or impacts from particles—or even the machine's control systems can induce decoherence, other errors in the quantum system, and unwanted interference and entanglement between the system's qubits. Qubits themselves are noisy, and adding more qubits to a system increases the system's noise.[28] Depending on the modality, some qubits are more susceptible to errors than other quantum modalities. All these factors can collapse a qubit, induce unintended entanglements, or create unintentional wavefunction interference that threatens the integrity of the information obtained by the qubit or a quantum system's process.

"Logical qubits" are groupings of qubits that correct for the faults induced by noise to help control for these errors and create fault-tolerant quantum systems. Rather than shielding and striving for perfect qubits, a fault-tolerant quantum system uses an overhead of qubits to correct quantum errors using various methods. One of the most common means of quantum error correction is to entangle many different qubits together to achieve one "noise-free" or "idealized" logical qubit.[29] Other approaches use parallel qubits to perform a range of tasks, such as spotting and correcting errors as they occur or simply executing a task thousands of times and then statistically determining the most probable solution.[30] The need to correct for errors is critically important for current "noisy intermediate-scale quantum" (NISQ) systems.[31]

The scale of quantum computers may remain limited until scientists are able to build clean, noise-free quantum systems or develop better fault-tolerant systems that can reliably solve large-scale computations without the high overhead of redundant, logical qubits.[32] It is also important to understand that a basic qubit is not analogous to a classical bit, not all qubits or their modalities are equal, and not all error correction techniques require the same volume of extra qubits. Scientists are still working through how to best and most efficiently correct for qubit errors. This means defense leaders should understand claims about quantum systems—especially quantum computers—and ask quantum computing program vendors about the logical qubit overhead.

Understanding the Modalities Used to Build Quantum Computers

Different quantum computing development teams use different hardware and control approaches—their modalities—to isolate, control, and manipulate their chosen qubits.[33] Quantum modality is also based on the type of particle a qubit uses. Qubits can be classified based on the primary particles that scientists use to build qubits: electrons, atoms, and photons.[34] Modalities matter because each of these qubit types has different properties and characteristics that affect the speed, accuracy, and overall performance of quantum computers. Moreover, the modality used will dictate the physical design of a quantum computer, which has real-world impacts on its utility.

- **Electron-based modalities.** There are two primary electron-based modalities: superconducting chips and quantum dot (also known as silicon spin). **Superconducting chips** exploit the unique properties of certain materials—typically aluminum—below specific threshold temperatures.[35] At temperatures that are colder than temperatures in outer space, these superconducting materials lose all electrical resistance, enabling scientists to access and control quantum behaviors.[36] **Quantum dots, also known as silicon spin**, are another electron-based qubit. While the infrastructure and chip manufacturing requirements of quantum dots are like superconducting circuits, they work differently. Whereas superconducting chips flow electrons in a circuit, quantum dots trap electrons on the chip in electrostatic wells between semiconductors that look like teeth on a comb.
- **Atom-based modalities.** The two major atom-based modalities are neutral (also referred to as cold) atom and trapped ion. Both modalities use lasers as key supporting technologies and do not require the cryostat or dilution refrigeration infrastructure of electron-based modalities. Atom-based modalities are also far more flexible, which expands their potential use cases and applications well beyond computation. The **neutral or cold atom** approach uses lasers to trap single atoms into a geometric, optical lattice. Lasers cool elemental vapors to de-excite the individual atoms to a temperature near absolute zero without allowing them to condense into a solid state.[37] Additional lasers are used to control and entangle atoms as well as apply gate functions. **Trapped ion** devices, similarly to neutral atoms, use elemental vapor inside ultra-high vacuum cells and lasers to strip the atoms of an electron to create an ion.[38] And like the neutral atom modality, trapped ion devices use lasers to entangle atoms and perform gate functions, either through careful use of a laser beam on multiple

stationary qubits simultaneously or by physically moving ions next to each other for adjacent operations.[39]

- **Photon-based modalities.** Photon-based modalities such as quantum optical circuits manipulate the polarization, or spin, of individual photons to encode information in a photonic qubit.[40] Photons are chargeless, massless particles of light. Photonic qubits are rapidly emerging as both a stand-alone modality and as a critical enabler of other modalities. Photons are already used in many digital information technology applications, conveying information through pulses of light. Photonic qubits—photons that are deliberately encoded with information or entangled with other photons—can move through fiberoptics as "flying qubits" or even travel through free space in laser light beams. Flying qubits are qubits that can physically travel from one place to another without decohering. Consequently, flying qubits are emerging as key to scaling quantum computers of any modality because they can network banks of quantum processors together.

Evaluating the performance of each modality's qubits

Key to exploiting quantum computers for defense is understanding how to measure the performance of their qubits. Since different modalities use different quantum particles for their qubits and approaches for manipulating them, there are also different ways to evaluate their performance. These differences can help define potential use cases for quantum computers in real-world battlefield applications.

Coherence times. In layman's terms, a qubit's coherence time is the lifetime of a qubit or the time it retains a quantum state. This matters because a quantum computer must be able to complete its computations before its qubits decohere and lose their encoded information. Depending on the modality, qubit coherence can last from fractions of a millisecond to a few seconds at most. Qubits are notoriously sensitive to magnetic or electric fields, radiation, heat, and even unintended "cross-talk" from other qubits in a quantum system. These influences can disrupt a qubit's state and interfere with and entangle it in ways that cause degradation and errors.[41]

Scalability. The power of a quantum computer is correlated with how many qubits to which it can scale. Some modalities are limited by the difficulties of facilitating qubit-to-qubit connectivity, but the biggest problem facing any quantum computer is qubit coherence and the sensitivity of their qubits to noise and other cross-talk.

Consistency of qubit production. The quality of a qubit and the consistency with which it can be produced will have an impact on the accuracy of a quantum computer. Quantum computers must be able to produce uniform qubits of a desired state if they are to accurately conduct gate operations or other functions. If, for example, several qubits in a computer began operations in a different state (spin up as opposed to down), they would process algorithms differently and distort the outcome.[42]

Controllability. A quantum machine must be able to control, manipulate, entangle, and conduct interference and logic gates on its qubits. Some qubit modalities lend themselves better to these operations than others.[43] Quantum dot qubits, for example, are difficult to entangle because they are physically isolated from other dots.

Gate speed. The speed of a gate function is crucial to ensure that a quantum computer can complete its program before its qubits decohere. If the qubits decohere before the function is completed, then the outcome will be in error. This is especially important as quantum computers scale to complete more difficult and longer algorithms.[44]

Modality Type	Benefits	Challenges
Superconducting Chips	Strong gate fidelity Can leverage existing microchip fabrication Small form / fit of chips similar to current semiconductor chips High gate speeds = faster processing times Circuit logic like classical computing	Requires cryogenic cooling Large infrastructure Large power requirements Short coherence times Scalability of individual quantum processors is limited—must be networked to increase processing
Silicon Spin / Quantum Dots	Strong gate fidelity Can leverage existing semiconductor technology High gate speeds = faster processing times	Requires cryogenic cooling Large infrastructure Large power requirements Short coherence times Limited demonstrated gate entanglement may imply inability to scale Vulnerable to interference / cross-talk
Neutral Atom	High controllability of individual qubits Stable, identical, and consistent qubits Strong connectivity across qubits Long coherence times (5”) Room temperature Excellent scalability	Low gate fidelity Slow gate speeds = slower processing times Need to miniaturize laser hardware Need to improve laser precision Need to increase vacuum cell quality
Trapped Ion	Stable, identical, and consistent qubits Strong connectivity across qubits Long coherence times (10”) Room temperature Excellent scalability High gate fidelity	Slow gate speeds = slower processing times Need to miniaturize laser hardware Need to improve laser precision Need to increase vacuum cell quality Ion charge may restrict scalability
Photonic	Promising qubit fidelity Long coherence times Can leverage existing microchip fabrication technologies Room temperature Are often used in conjunction with atom-based modalities Can be used to convey quantum information (“flying qubits”) from one physical location to another	Massless photons are difficult to control Photons do not naturally interact, resulting in poor gate operations High qubit (photon) loss rates (signal loss) Poor qubit connectivity Difficult to entangle Difficult to scale

Table 1: A summary of the different quantum modalities and their relative strengths and challenges for quantum computing.

Credit: Heather Penney/Mitchell Institute.

Gate fidelity. Gate fidelity refers to the accuracy, reliability, and repetition with which a quantum gate can control and manipulate qubits in a system.[45] This can also be understood as the difference between the ideal mathematical outcome and the real, physical outcome of the operation. The physical methods, such as lasers, charge, or magnetic flux, used to conduct gate operations on real quantum devices can be imperfect, and this may induce errors and inaccurate outputs.[46]

Each quantum modality has its own unique advantages and challenges, which may define its potential operational use cases and subsequent technical development.[47] In addition to the performance metrics of a system’s modality, U.S. defense leaders must keep the demanding environment of combat operations in mind when assessing what modalities to pursue. Traditional computer constraints of size, weight, power, and cooling on specific weapon systems may trump performance metrics when considering what quantum modalities are pragmatic to mature and field and determining use cases. For instance, how will the massive infrastructure demands of cryogenic superconductors fit into real-world operational concepts, particularly agile combat employment? In some cases, large, exquisite quantum computers using electron-based modalities may be best suited for performing cloud-type operations or other tasks at fixed bases where they can be supported and defended, while trapped ion or neutral atom approaches may be more appropriate for scaled-down capabilities that are more deployable or relocatable. As with any technical design, senior leaders should understand the tradeoffs between capability, cost, complexity, size, and operational utility of quantum modalities so they may appropriately focus research and development efforts. Importantly, they should judge the performance of a modality based on the needs of the intended application.

Senior leaders should understand the tradeoffs between capability, cost, complexity, size, and operational utility of quantum modalities so they may appropriately focus research and development efforts. Importantly, they should judge the performance of a modality based on the needs of the intended application.

Different types of quantum computers

Senior leaders should be aware that different types of quantum computers are not interchangeable.[48] Each type of quantum computer is best suited for specific applications, and understanding the differences between them will inform resourcing and programmatic decisions for different warfighter use cases.

- **Quantum emulators.** Despite the name, quantum emulators are traditional, binary computers that *simulate* quantum computers using probability and statistics and do not use quantum mechanics. Some in the industry describe their quantum emulators as quantum simulators or quantum circuit simulators, although true quantum simulators use qubits.[49] Emulators are useful for testing and validating different quantum computer designs as well as developing quantum algorithms. These classical emulators are limited in scale because they cannot model more than 60 qubits.[50]
- **Quantum simulators.** Quantum simulators are quantum-based devices of any modality type (neutral atom, superconducting chips, etc.) that use qubits and other quantum effects to validate the accuracy of mathematical models of complex physical systems.[51] Classical computers are unable to simulate many of these problems, processes, or interactions because they are just too complex, voluminous, and have too many variables.[52] Although current quantum simulators have only generated models of individual molecules, more advanced simulators will describe the behaviors of the real, physical world well enough to dramatically impact the material sciences, pharmaceutical industry, weather and climate sciences, energetics, and even quantum behavior.
- **Quantum annealers.** Quantum annealers are superconducting chip-based quantum computers that do not use logic gates—a type of physical function that can have multiple inputs and a single output—that are the basic blocks of digital computing systems. Instead, quantum annealing machines use couplers to entangle qubits and create interference between wavefunctions through chip design and layout, referred to as "topology."[53] Annealing machines energize the circuits (waveforms) through magnetic fields

and then allow the qubits to naturally relax to their lowest energy state, which represents the solution.[54] This unique approach to combining wavefunctions makes annealers very efficient at specific types of optimization problems, like composing military missions and planning fuel expenditures, as well as probabilistic sampling, which can be useful for machine learning.[55]

- **Universal quantum computers.** A universal quantum computer processes information through quantum logic gates, which can be combined in any sequence to run increasingly complex algorithms.[56] Quantum computers cannot run traditional logic gates because doing so would collapse their waveforms and lose information. Quantum gates can manipulate qubits without measuring their state, are fully reversible, and preserve the qubits' quantum properties until they decohere or are deliberately measured. Any of the quantum modalities can be used to build a universal quantum computer, and each modality has its own benefits and limitations. The architecture of universal quantum computer processing requires more qubits than a quantum annealing computer does, but universal computers can also solve for a wider variety of algorithms than annealers, making universal computers more broadly useful than other types of quantum computers.[57]

Building a pragmatic quantum computer

The state of quantum computing is still in its early stages. In 2000, theoretical physicist David P. DiVincenzo proposed seven conditions that must be met to field a useful universal quantum computer.[58] "DiVincenzo's criteria" are a useful means for U.S. defense leaders to understand how far potential computer systems have progressed as well as the specific types that are in development. DiVincenzo's intention was to move the focus away from experimentation and toward a practical quantum device: "I always said that in some sense, these criteria are exactly the ones that you would teach to kindergarten children about computers, quantum, or otherwise."[59] These criteria are widely accepted throughout the quantum computing field, provide technologists with specific engineering objectives, and are also a means to evaluate different quantum computing designs:

1. **A scalable physical system with well-characterized qubits.** The system must be able to expand to a larger number of qubits without significant difficulty while retaining qubits whose properties can be precisely controlled, maintained, and measured. This requires systems to control increases in noisiness and unruliness as the absolute number of qubits grows, and it requires infrastructure, power, and support mechanisms that are practical.
2. **The ability to initialize qubits in a known state.** Qubits must begin in a known state if the outcomes of a quantum system's computational processes are to be accurate. This means a quantum system must be able to prepare qubits in a specific, known state to facilitate the accurate processing of quantum algorithms.
3. **Long, relevant coherence times.** Qubits must be able to maintain their quantum state and coherence through gate manipulation and long enough to complete the quantum computation accurately and then be measured. As algorithms expand in length, qubits must remain faithful and coherent for the duration of the process. Otherwise, the quantum system risks an erroneous outcome for the computation.

4. **A "universal" set of quantum gates.** Algorithms use logic gates to instruct how a computer should process an equation. A universal quantum computer must be able to implement any quantum algorithm using the same set of logic gates that any other quantum computer may also use—in other words, software programmers should not have to "rewrite" the same algorithm for each type of quantum computer. This requirement speaks to the ability of any universal computer to share the same algorithm.
5. **A qubit-specific measurement capability.** The system must be able to measure the state of individual qubits with high accuracy during a computing process and for the output of the final state of the computation. Some quantum algorithms will require intermediate results, but qubit error correction will also demand quality control applications to facilitate the final readout.

The last two DiVincenzo criteria are useful for assessing the potential for quantum processors to communicate with each other.[60] Quantum communication is critical to scaling quantum computation—by networking banks of quantum processors together, for example, to increase total computing capability.

6. **The ability to interconvert stationary and flying qubits.** A scalable quantum processor should be able to accurately convert between stationary qubits (used for gate operations) and flying qubits (that physically move between different parts of the system for communication) and back again.
7. **The ability to faithfully transmit flying qubits between specified locations.** A scalable quantum processor should also be able to move qubit information between two locations without collapsing the qubit or causing it to lose its state or coherence.[61]

Quantum computers are still early in their development, and policymakers should be educated consumers of these technologies. But because quantum computers are so very different from classical computers and each other—across qubit types and their quality, quantum modality, computer types, and even the architecture of the computer design—U.S. policymakers and senior defense leaders need a consistent and widely accepted set of metrics to compare apples to oranges.

Current measures for the quality of a quantum computer

Quantum scientists recognize that senior leaders and other decision-makers need metrics by which they can compare computational quality across different types, modalities, and qubits and have proposed several measures to compare computational quality across the different modality and hardware approaches. Quantum computing, however, is still so nascent that there are competing proposals to measure capacity and quality.

- **Absolute qubit count.** The total number of qubits in a computer is not a good measure by which to compare quantum computers. Different qubit modalities and even different qubit manufacturing quality can dramatically impact the error rates of a qubit. Moreover, scaling qubits to create more powerful computers actually induces more noise into the quantum system. This can be from the inherent noisiness of the qubit or the increased control systems used to manage and coordinate qubit behavior. Regardless of the cause, more noise means more errors.[62] Quantum scientists and senior leaders need a better way to measure the capacity and quality of quantum computers.

- **Quantum volume.** One of the most widely accepted methods of assessing quantum computers is quantum volume. This is a single number that measures the complexity of a quantum computer. Volume is measured by taking the number of qubits, the number of gates in the circuit (circuit depth), and the connectivity, all controlled for error rates.[63] Generally speaking, the larger the volume number, the more complex the problems the quantum computer can solve. Other quantum volume definitions simplify this measure to the largest square circuit—where width (number of qubits) and depth (number of gates) are equal—that can be run on a quantum computer before the qubits decohere.[64] As an example, the Quantinuum System Model H1-1 is a 20-qubit system that achieved a quantum volume (QV) of 2^{19} in June 2023.[65]
- **Algorithmic qubits.** Algorithmic qubits are another quantum volume measure based directly on logical qubits, not absolute qubits.[66] Intended to be a proxy for the ability to execute real quantum algorithms, this metric mirrors quantum volume but prioritizes practical algorithms in its measure of circuit depth, not randomized gates that maintain fidelity.[67] These algorithms are benchmarked through industry consortiums such as the Quantum Economic Development Consortium (QED-C) and are expected to evolve as the field matures.[68] As such, the algorithmic qubit measure includes the version number, as this is a reference to the set of algorithms used in the assessment and is time-relevant. For example, IonQ achieved 29 algorithmic qubits (#AQ) in October of 2023.[69]
- **Circuit layer operations per second (CLOPS).** CLOPS is a way to evaluate the processing speed of a quantum computer. Different modalities and qubits have different gate speeds, so circuit layer operations per second (CLOPS) is a proposed means for understanding how fast a quantum computer can solve algorithms—also known as quantum runtime—across computers that share similar quantum volumes.[70] When processing speed matters, CLOPS can provide senior leaders with an additional evaluation criterion.

Progress in quantum computing benchmarks, controls, & interfaces is still needed

Benchmarks to measure quantum computer performance in the real world are needed

The above proposals for measuring capacity and quality are an excellent start for evaluating the hardware of quantum computers of different modalities and qubit count, but they ultimately fall short in measuring real-world performance. Even as engineers work to scale quantum computers, they do not agree on what size, volume, quality, or configuration of quantum computer is needed to field a minimum viable capability—and what kinds of problems that computer would be able to solve.[71]

Quantum computers are varied and complex, and the manner of their computing is not straightforward; there are many elements linked to the performance and quality of the quantum device. Moreover, different applications (simulation versus factorization, for example) require different quantum configurations.[72] Because of the many modalities and hardware approaches that companies are using to pursue their development of quantum computers, there is a need to establish benchmarks that enable a standardization of performance evaluation.[73] The Defense Advanced Research Projects Agency (DARPA), the QED-C, and other leading industry members are pursuing the development of these benchmarks to better understand what is minimally necessary for quantum computers to be useful for specific applications at specific scales.[74] Establishing benchmarks would also enable a valid and useful "apples-to-oranges" comparison across different quantum modalities, applications, and the operational potential of different quantum computer designs.

Advancements in classical control systems are still needed to interface with quantum computers more effectively

Quantum computers cannot operate without the controls and interfaces provided by classical technologies. A major challenge that engineers face in developing pragmatic quantum computers is the incompatibility between quantum and classical computers. Control devices that are "noisy" or unsynchronized can distort a qubit, adding to the qubit overhead required to correct for faults. The precision and speed of these control electronics have an impact on the quality and accuracy of quantum solutions.[75] For example, superconducting computers will require classical electronic and cryo-controls that can work across multiple temperature domains.[76] The careful orchestration of signal, timing, and operations of classical devices are necessary to control, measure, and read out quantum computations, and as scientists and engineers work to scale quantum computers of any modality, these classical electronics will change.[77] There currently remains a gap between classical technology and what is needed for future fault-tolerant, universal error-corrected quantum processors.[78]

The hype that surrounds quantum is understandable—but not helpful. Senior U.S. defense leaders should have a basic understanding of the science, the challenges, and the nuances of fielding a useful quantum computing device if they are to make wise choices about how to ensure and secure the development of a quantum advantage.

Conclusion

Senior U.S. defense officials should understand these basics of quantum computing so they may make prudent and insightful choices regarding how to direct and resource DOD programs while also leveraging the rapid developments of the commercial industry. Not all quantum computers are equal: each modality, qubit type, and computer design has its own special attributes and strengths, and commercial development choices may not always align with U.S. military use cases, problems, and operational scenarios. Senior U.S. defense leaders should closely monitor and leverage commercial investments while simultaneously pursuing technological approaches that may have more military-unique applications. Moreover, policymakers and program managers should likewise understand that not all quantum computers are equal. Instead, they must use their knowledge of the science to evaluate the quality and overhead of the qubits, as well as their experience and insight into planning and operations to determine how well the design can integrate with other military capabilities. These are specialized machines that will not replace traditional, binary computers but will augment them to provide key computational and strategic advantages to U.S. national security.

Given the potential for quantum computing to transform or even revolutionize key elements of U.S. national power and global dynamics, the hype that surrounds quantum is understandable—but not helpful. Senior U.S. defense leaders should have a basic understanding of the science, the challenges, and the nuances of fielding a useful quantum computing device if they are to make wise choices about how to ensure and secure the development of a quantum advantage. Importantly, quantum experts and DOD leaders must bring together their respective knowledge, experience, and understanding—regarding the technologies, the operational landscape, and use cases—to establish practical metrics for assessing different modalities and types of quantum computers. Without a method to weigh the potential of this game-changing capability, the full benefit of quantum computing might not be realized for U.S. national security. ✪

Endnotes

1 Michael E. O'Hanlon, *A retrospective on the so-called revolution in military affairs, 2000-2020* (Washington, DC: Brookings Institution, September 2018).

2 Ari Joury, "Will Quantum Computers Replace Their Classical Counterparts?" Built In, January 23, 2021; "Quantum Computing: How it differs from classical computing?" BBVA, December 10, 2019; and ATARC Quantum Working Group, "Applied Quantum Computing for Today's Military," Advanced Technology Academic Research Center (ATARC), May 2021.

3 Charles Choi, "Two of World's Biggest Quantum Computers Made in China," *Spectrum*, IEEE, November 26, 2021; and François Candelon, "The U.S., China, and Europe are ramping up a quantum computing arms race. Here's what they'll need to do to win," *Fortune*, September 2, 2022.

4 Emily Conover, "Google claimed quantum supremacy in 2019—and sparked controversy," *Science News*, December 16, 2019; Jamilah Lim, "China's quantum computing efforts surpasses the West's—again," *Tech Wire Asia*, November 3, 2021; and Office of the Secretary of Defense (OSD), *Military and Security Developments Involving the People's Republic of China 2022*, annual report to Congress (Washington, DC: DOD, October 26, 2022).

5 "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," The White House, May 4, 2022.

6 Dominic Walliman, "The Map of Quantum Computing - Quantum Computing Explained," *Domain of Science* on YouTube, December 3, 2021.

7 "Quantum Programming - Part 1," *New Mind* on YouTube, August 5, 2022.

8 Interview with Lamar Silves, June 5, 2023.

9 "Quantum Computing Enables Unprecedented Materials Science Simulations," U.S. Department of Energy, August 4, 2021.

10 Frank Phillipson, "Quantum Machine Learning: Benefits and Practical Examples," CEUR Workshop Proceedings vol. 2561, February 2020; "Quantum Machine Learning Explained," *IBM Technology* on YouTube, October 19, 2022; and "Quantum Machine Learning MOOC," *Quantum ML* on YouTube, updated April 26, 2021.

11 Kevin Townsend, "Solving the Quantum Decryption 'Harvest Now, Decrypt Later' Problem," *Security Week*, February 16, 2022.

12 Joury, "Will Quantum Computers Replace Their Classical Counterparts?"

13 For more on DOD's efforts in the cislunar regime, see Charles Galbreath, *Securing Cislunar Space and the First Island Off the Coast of Earth* (Arlington, VA: The Mitchell Institute of Aerospace Studies, January 2024).

14 "1953: Transistorized Computers Emerge," Computer History Museum. The very first computers used vacuum tubes—transistors were the next evolution that decreased size and power requirements while increasing computation speeds. Next generations of computer hardware would use integrated circuits and microprocessors. Advances in material science and physics have since enabled the rapid and dramatic improvement of microprocessors that many people understand as "Moore's law": that the number of transistors on an integrated circuit would double every two years. The primary means of achieving this has been through making smaller and smaller transistors. There may be reason to believe that there are physical and practical limits to Moore's Law. Current silicon chips can be etched at a 10 nanometer scale (although most are between 13 and 17 nm due to cost/value tradeoffs); at approximately 7 nm, the scale of computation begins to edge into the quantum realm and the principles of classical physics that drive classical computers begin to break down. Some chip designers, however, are exploring 3-dimensional chips, which may offer new advantages to classical computing. Alex Hughes, "What is Moore's Law and is it still relevant today?" *BBC Science Focus*, May 2022; and Heidi Vella, "Quantum for dummies: the basics explained," *Engineering and Technology*, updated October 9, 2023.

15 "Quantum Programming - Part 1."

16 Stephanie Pappas, "Scientists See Quantum Interference between Different Kinds of Particles for First Time," *Scientific American*, January 11, 2023.

17 David Morin, "Introduction to Quantum Mechanics," in *Waves*, draft book (n.d.).

18 Gavin Wright, "Quantum Interference," Tech Target, updated February 2023.

19 "What Is Entanglement and Why Is It Important?" *Caltech Science Exchange*.

20 Paul Sutter, "What is quantum entanglement?," *Live Science*, May 26, 2021.

21 "Nonlocality and Entaglement," The Physics of the Universe; and Olimpia Lombardi and Dennis Dieks, "Modal Interpretations of Quantum Mechanics," *Stanford Encylopedia of Philosophy*, revised October 8, 2021.

22 "What Is Entanglement and Why Is It Important?" Physicists do not say "counterclockwise," they use the term "anticlockwise."

23 "Quantum Programming - Part 1."

24 Walliman, "The Map of Quantum Computing - Quantum Computing Explained."

25 Walliman, "The Map of Quantum Computing - Quantum Computing Explained."

26 This definition or use of modality—the physical methods used to isolate, control, and manipulate particles—is not to be confused with modal interpretations of quantum theory that "assigns

definite properties to physical systems even when no measurements are taking place." Scientists do not have a good theoretical explanation as to why wavefunctions collapse, and the modal interpretation is one way to grapple with the broader philosophical implications of quantum physics. For a summary of modal interpretations of quantum theory, see "Modal Interpretations of Quantum Mechanics."

27 Walliman, "The Map of Quantum Computing - Quantum Computing Explained."

28 Zeyuan Zhou et al., "Quantum Crosstalk Robust Quantum Control," November 20, 2022.

29 Walliman, "The Map of Quantum Computing - Quantum Computing Explained."

30 "Logical qubits start outperforming physical qubits," Quantinuum, August 4, 2022.

31 Kishor Bharti et al., "Noisy intermediate-scale quantum (NISQ) algorithms," *Review of Modern Physics*, October 6, 2021.

32 Bharti et al., "Noisy intermediate-scale quantum (NISQ) algorithms,"; and Alexandru Paler and Simon J. Devitt, "An introduction to Fault-tolerant Quantum Computing," DAC '15 Proceedings of the 52nd Annual Design Automation Conference, Article no. 60, August 15, 2015.

33 Dominic Walliman, "Who Has The Best Quantum Computer?" *Domain of Science* on YouTube, January 29, 2022.

34 "Quantum Computing Hardware - An Introduction," *Verve Ventures* on YouTube, December 2, 2021.

35 Temperatures typically reached by leading superconducting quantum computers reach as low as 1 milliKelvin. For comparison, deep space – as in, outer space beyond our solar system – has been measured to be 2.7 milliKelvin. "How cold is it in outer space?," *Astronomy*, February 28, 2020.

36 Cooper pairs are entangled electrons whose total value is a whole integer (wavefunction). JR Minkel, "Splitting Up Cooper Pairs," *Physics Review*, Focus 9, 33, June 28, 2002. Classical chips flow electrical energy—electrons—through circuits in on-off logic gates, but the cost of the resistance, or friction, in the metal is heat and even loss of electrons. This kind of "noise" can result in error, and classical chips monitor voltage and even add in electrons to control for errors. A room-temperature quantum chip cannot control or correct for errors in this way because the superposition of the electron would collapse during measurement. "Building a quantum computer with superconducting qubits (QuantumCasts)," *TensorFlow* on YouTube, February 17, 2019. Aluminum is a commonly used superconductor. Hans Mooij, "Superconducting quantum bits," *Physics World*, December 1, 2004.

37 Much like an active noise-canceling headset, the frequency of a laser can be tuned to counter the natural frequencies of the atom, thereby cooling and stilling the atom, making it easier to trap and move. "Building Scalable Quantum Computers from Arrays of Neutral Atoms," *Atom Computing* on YouTube, May 11, 2022.

38 For a more in-depth description of how trapped ion devices work, see Gabriel Mintzer, "Introduction to Trapped-Ion Quantum Computing," MIT 6.s089—Intro to Quantum Computing, February 2, 2020.

39 John Timmer, "Honeywell releases details of its ion trap quantum computer," *Ars Technica*, April 7, 2021.

40 For an excellent overview of the mechanics and state of quantum photonics, see Galan Moody et al., "2022 Roadmap on integrated quantum photonics," *Journal of Physics: Photonics*, January 31, 2022.

41 "Cross-talk" is a term for when control signals of quantum applications spill over to or are nabbed by unintended qubits. Cross-talk effectively pollutes the control of the quantum application and creates errors. "Combatting crosstalk in quantum computers," Universtiy of Waterloo, October 23, 2021; and Katherine McCormick, "Decoherence Is a Problem for Quantum Computing, But ..." *Scientific American*, March 30, 2020.

42 "Scalable manufacturing processes for quantum computing," *Nature Electonics*, April 6, 2022.

43 Karen Wintersperger et al., "Neutral Atom Quantum Computing Hardware: Performance and End-User Perspective," *EPJ Quantum Technology*, August 28, 2023.

44 Riken, "Scientists achieve key elements for fault-tolerant quantum computation in silicon spin qubits," *Phys.org*, January 19, 2022.

45 Monica Hernandez, "Breakthrough in quantum universal gate sets: A high-fidelity iToffoli gate," *Phys.org*, May 24, 2022.

46 "What does quantum gate fidelity mean?" Quantum Computing, Stack Exchange, edited May 12, 2022.

47 "Quantum Computing Hardware - An Introduction."

48 A simple definition of a quantum computer is a device that uses quantum phenomena such as superposition and entanglement to perform calculations, but it should be clear that this definition is very inclusive and may be far broader than some policymakers would expect, based on their experience with modern, classical computers. "Quantum Annealer vs Universal Gate Based Quantum Computers | Is D-Wave a Real Quantum Computer?" *Anastasia Marchenkova* on YouTube, February 16, 2021.

49 Emulators have a place in supporting design efforts of quantum computers, and can provide accessible and affordable platforms for quantum algorithm and programming development and training. See, for example, "qsim:Optimized quantum circuit simulators," Quantum AI, Google.

50 Emulators use statistical methods, Monte Carlo methods, and density functional theory to model quantum systems. Emulators are limited in the size of what they can simulate because of the exponential complexity as the quantum simulation scales. The more precise or accurate the needed outcome, the fewer qubits an emulator can simulate because of that limitation. Dominic Walliman, "Quantum Simulation Explained in 9 Slides," *Domain of Science* on YouTube, December 11, 2020.

51 Tomi Johnson, Stephen Clark, and Dieter Jaksch, "What is a quantum simulator?" *EPJ Quantum Technology*, July 23, 2014.

52 Walliman, "Quantum Simulation Explained in 9 Slides."

53 "Quantum Annealer vs Universal Gate Based Quantum Computers | Is D-Wave a Real Quantum Computer?"

54 "Quantum Annealing," *Quantum Computing at Davis* on YouTube, May 28, 2021; and Dominic Walliman, "How The Quantum Annealing Process Works," *D-Wave* on YouTube, December 15, 2015.

55 "Quantum Annealer vs Universal Gate Based Quantum Computers | Is D-Wave a Real Quantum Computer?"

56 "Quantum Logic Gates," National Institute of Standards and Technology (NIST), updated January 25, 2024; and Moritz Fink, "10 Quantum Gates You Need To Know For Quantum Computing," *Medium*, October 17, 2020.

57 The need to error-correct as absolute qubit count grows is a major scaling challenge to universal computers. Increasing the complexity and duration of algorithm operations increases noise, cross-talk, and demands more of coherence times.

58 David P. DiVincenzo, "The Physical Implementation of Quantum Computation," IBM, April 13, 2000.

59 Iulia Georgescu, "The DiVincenzo criteria 20 years on," *Nature Reviews Physics*, November 3, 2020.

60 DiVincenzo, "The Physical Implementation of Quantum Computation."

61 DiVincenzo, "The Physical Implementation of Quantum Computation"; "What is the DiVincenzo Criteria?" Wayne State University, Mike Ilitch School of Business; and Hamed Nazari, "DiVincenzo Criteria," QuantumEon, March 9, 2023,

62 This challenge of scaling qubits but also avoiding the concurrent noise growth of adding more qubits is a concern for many technologists, some of whom have speculated that there may be an inherent limitation on the number of absolute qubits different quantum computers may be able to host. See "Don't fall for quantum hype," *Sabine Hossenfelder* on YouTube, February 6, 2021.

63 Andrew W. Cross et al., "Validating quantum computers using randomized model circuits," *Physical Review A*, September 20, 2019.

64 Qiskit, "What Is Quantum Volume, Anyway?" *Medium*, August 20, 2020.

65 "Quantinuum H-Series quantum computer accelerates through 3 more performance records for quantum volume: 217, 218, and 219," Quantinuum, June 30, 2023.

66 Emil Protalinski, "IonQ's roadmap: Quantum machine learning by 2023, broad quantum advantage by 2025," *VentureBeat*, December 9, 2020.

67 Larry Dignan, "IonQ introduces Algorithmic Qubits to counter Quantum Volume in quantum computing," *ZDNET*, December 9, 2020.

68 "Algorithmic Qubits: A Better Single-Number Metric," IonQ, updated January 18, 2024.

69 Matt Swayne, "IonQ Achieves 29 Algorithmic Qubits On Barium Platform," *The Quantum Insider*, October 24, 2023.

70 "Driving quantum performance: more qubits, higher Quantum Volume, and now a proper measure of speed," *IBM Research Blog*, November 1, 2021.

71 "Quantum Benchmarcking," DARPA.

72 Matt Langione et al., "The Race to Quantum Advantage Depends on Benchmarking," Boston Consulting Group, February 23, 2022.

73 Chris Coleman, "A Guide To Quantum Computing Benchmarking And Certification," *The Quantum Insider*, August 12, 2022.

74 "DARPA announces contracts to Raytheon BBN & to USC for Quantum Benchmarking Program," *Inside Quantum Technology News*, March 8, 2022; and "Benchmarking our Next-Generation System," IonQ, October 18, 2021.

75 Carrie A. Weidner et al., "Applying classical control techniques to quantum systems: entanglement versus stability margin and other limitations," Quantum Physics on ArVix, July 25, 2022.

76 Monica Hernandez, "Quantum Computing Workshop Brings Classical Control Systems Into Focus," AQT, December 20, 2022.

77 Tracy Marc, "New control electronics for quantum computers that improve performance, cut costs," *Phys.org*, May 3, 2022.

78 Hernandez, "Quantum Computing Workshop Brings Classical Control Systems Into Focus."

About The Mitchell Institute

The Mitchell Institute educates broad audiences about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Series

The Mitchell Institute Policy Papers present new thinking and policy proposals to respond to the emerging security and aerospace power challenges of the 21st century. These papers are written for lawmakers and their staffs, policy professionals, business and industry, academics, journalists, and the informed public. The series aims to provide in-depth policy insights and perspectives based on the experiences of the authors, along with studious supporting research.

For media inquiries, email our publications team at
publications.mitchellaerospacepower@afa.org

Copies of Policy Papers can be downloaded under the publications tab on the Mitchell Institute website at
https://www.mitchellaerospacepower.org

About the Author

Heather R. Penney is a senior resident fellow at the Mitchell Institute, where she conducts research and analysis on defense policy, focusing on the critical advantage of aerospace power. Prior to joining Mitchell Institute, Penney worked in the aerospace and defense industry, leading budget analysis activities, program execution, and campaign management. An Air Force veteran and pilot, Penney served in the Washington, DC Air National Guard flying F-16s and G-100s and has also served in the Air Force Reserve in the National Military Command Center.

An Affiliate of the Air & Space Forces Association | www.mitchellaerospacepower.org