Vol. 46, January 2024

MITCHELL INSTITUTE
Policy Paper

Key Points

In the past century, America achieved and maintained military dominance by exploiting technologies to gain a capability overmatch against numerically superior adversaries. Yet, current U.S. technological leadership is diminishing in key areas, including quantum information science and technologies (QIST).

Quantum science has the potential to fill certain capability gaps that warfighters are likely to face in a peer conflict, such as navigation, timing, sensing, and more.

Senior leaders need a foundational understanding of quantum science to assess the maturity of these technologies and focus resources on the development and fielding of high-potential, high-payoff capabilities.

Scientists and engineers manipulate, control, and measure quantum particles through different means called modalities. Different modalities, such as superconducting chip, neutral atom, trapped ion, or photonic qubit, each have unique benefits, limitations, and possible use cases.

Meeting future requirements and understanding emerging threats will require Department of Defense and service leaders to understand how these modalities translate outside of the laboratory and into the development of pragmatic combat capabilities.

China has shown a substantial, long-term commitment to working through and solving many of the scientific and engineering problems associated with fielding robust and rugged quantum capabilities.

Without a foundation of knowledge in quantum sciences, senior leaders risk failing to understand the strategic and operational implications of Chinese QIST developments and demonstrations.

The Quantum Advantage: Why it Matters and Essential Next Steps

Part 1: Understanding the Science to Make the Right Choices

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

Abstract

In the past century, America achieved and maintained military dominance by exploiting technologies to establish a capability overmatch against numerically superior adversaries. Accomplishing this meant leveraging revolutions in the advancement of technology. Today's revolution in quantum information science and technologies (QIST) presents a similar opportunity for the Department of the Air Force and elements of the broader Department of Defense.

However, senior leaders need better guidance to meaningfully evaluate QIST applications, as they are not intuitive or comparable to other modern technologies. Without a basic grasp of the science, leaders are ill-equipped to understand the use cases they are presented, ask the right questions, or make effective resourcing decisions.

This paper provides senior decision-makers with an accessible, operationally focused primer to understand the principles of quantum science as a baseline for how QIST may be applied to use cases in the battlespace. It describes quantum behaviors and the methods scientists and engineers use to control and measure quantum particles. The second paper in this series explores the potential of quantum computing. The third paper in this series focuses on how to cultivate the quantum defense industrial base to provide U.S. warfighters a quantum advantage in a peer conflict.

A baseline understanding of quantum principles is necessary for decision-makers to sort through the hype of the QIST revolution and recognize the true potential of these emerging capabilities to secure a quantum advantage against China. Moreover, this foundation of knowledge will enable senior leaders to understand the operational implications and strategic consequences of Chinese QIST demonstrations.

Introduction

Since the Second World War and the birth of atomic power, America established military dominance by exploiting technologically advanced capabilities to establish overmatch against numerically superior adversaries. The explicit pursuit of gaining a technological edge over the Soviet Union was the premise of the "Second Offset" strategy of the 1970s and 1980s, in which the U.S. Department of Defense (DOD) accelerated efforts to develop capabilities such as stealth, precision navigation and timing, precision weapons, improved datalinks and communication, advanced sensors, and greater computer processing to yield dramatic synergies for successful combat outcomes. Maintaining such a technological advantage matters even more to national security today, yet the United States no longer maintains the scientific and manufacturing primacy that it enjoyed during the Cold War. To regain a technological lead and secure a military advantage, DOD leaders identified quantum information science and technologies (QIST) as a principal "Third Offset" investment.[1] The United States is not alone in this endeavor: China is also demonstrating a commitment to develop advanced quantum technologies. This obviously stands as a major concern.

The value of establishing an early technological "leap ahead" advantage over an adversary is clear. The Second Offset strategy's advanced sensing, combined with tactical datalinks, enabled forces to share their situational awareness across the battlespace and empowered battle managers and mission commanders to make better decisions and apply their limited forces more effectively. Stealth enabled key missions to evade detection by adversary air defenses or fighters, changing traditional attrition calculus and seizing the initiative of surprise. GPS and precision-guided munitions, whether GPS- or laser-guided bombs, decreased the number of weapons necessary to achieve desired effects against targets.[2] The value of this technological overmatch was demonstrated in the spectacular performance of the U.S. Air Force in the air campaign in Operation Desert Storm and subsequent operations.

However, Chinese and Russian military leaders observed this success as well, and both spent the following decades developing strategies and capabilities to overcome these advantages. This is particularly true of China, with the aspiring superpower developing and fielding advanced military capabilities that once belonged exclusively to the United States. Moreover, China has also developed capabilities designed to render key U.S. systems ineffective, such as advanced integrated air defenses, long-range cruise missiles, counterspace capabilities, and fifth-generation stealth aircraft. To achieve this, China focused on rapidly developing its own domestic engineering talent and industrial base by exploiting U.S. academic relationships to accelerate their access to leading scientific discoveries, leveraging technology transfer and other data rights to onshore engineering and manufacturing capabilities, and investing in technology companies to gain access to important engineering advances—in other words, through academic and economic espionage.[3] In recent years, these efforts extended to QIST, and Chinese investment and advancements in this area now outpace the West.[4] Their achievements have understandably alarmed U.S. defense leaders.

At a macro level, DOD leadership now realizes the value of successfully fielding quantum applications both before our adversaries and before they can develop countermeasures. Like stealth and precision strike complexes, QIST capabilities could deliver a lasting military primacy that bolsters U.S. deterrence. Quantum timing and navigation, for example, could replace dependencies on space-based GPS; quantum sensing could enhance ISR and kill chains; and quantum computation could decrypt encoded messages or enhance machine learning.

While it is one thing to recognize the importance of QIST, it is also important to recognize the risk of ceding that capability advantage to an adversary. Senior leaders should understand this quantum revolution as analogous to the opportunity that the emergence of semiconductors and microelectronics presented. While DOD officials could not have foreseen all the applications and capabilities that these technologies would mature into, they did understand that semiconductors and microelectronics had the potential to radically transform warfighter capabilities. Indeed, U.S. leadership in this industry gave the United States and its allies a technological edge in processing, information technologies, and advanced software programming that endured for nearly four decades. QIST presents just such a similar revolution today.

This is a Department of Defense-wide challenge, with QIST impacting all the services. However, it is particularly relevant for the Department of the Air Force, given how critical capabilities such as navigation, timing, sensing, and spectrum control are to Air Force mission sets—missions that joint and coalition operations depend on. Leaders must consider this as they prioritize long-term and near-term quantum technology investments needed to mature this field and outpace adversary progress.

As a first step, it is important for Department of Defense and Air Force leaders to master a basic working understanding of

What is Quantum?

"Quantum" broadly refers to sub-atomic particles and their attributes and behaviors. Engineers have long leveraged quantum principles to develop well-known technologies such as lasers, MRI machines, and atomic clocks. What is revolutionary about QIST today is the ability to directly and precisely control, manipulate, and measure quantum particles, attributes, and behaviors.

The ability to encode and process information using quantum bits, or qubits, creates incredible computation potential, but senior leaders must also be aware that quantum computers are not simply "super-fast supercomputers." Instead, they should be understood as specialized computers that can solve specialized problem sets, such as complex optimization problems or molecular modeling, that current computers cannot. Quantum computers may also be more efficient and faster at highly complex artificial intelligence/machine learning algorithms, but there are also many use cases where classical (or traditional) binary computing delivers faster and more accurate solutions.

The ability to precisely control quantum particles and behaviors creates opportunities for additional applications—and these are closer to fielding as real capabilities than useful quantum computers. Timing that is a million times more precise than current atomic clocks, gravimeters and magnetometers for sensing applications, and highly sensitive all-band radio frequency receivers are just a few examples.

Senior leaders should also understand that to field pragmatic quantum capabilities, they must develop the supporting classical control and interfacing technologies. Improved photonics, miniaturized lasers, ultra-high vacuum cells, and even classical computers that integrate quantum with current and future weapon systems cannot be neglected if the DOD is serious about moving quantum out of the laboratory and into the battlespace.

QIST and its potential applications to make smart resource decisions that will meaningfully accelerate the fielding of pragmatic and game-changing quantum-based military capabilities. Given the complexity and counter-intuitive nature of quantum science, it can be difficult to decipher between achievable near-term QIST goals and what long-term investments might yield. It is also challenging to define the possible range of unanticipated applications or recognize what claims about the technology might be an overreach or even pure science fiction. Some applications may make sense in the lab but would not transfer well to operational employment. The promise to transmit data across undetectable datalinks, render classical computers irrelevant, send information faster than the speed of light, or detect stealthy aircraft is alluring for senior leaders who seek to realize an operational quantum advantage. Senior leaders should understand enough of the science behind QIST to sort the real from the hype.

This white paper, the first of three, seeks to provide leaders with a foundation of knowledge regarding the basics of quantum science; the means, or modalities, that scientists use to control and manipulate quantum particles; and the applied technologies that advances in quantum science have made possible. This foundation is essential for understanding how quantum applied technologies work and for evaluating potential operational use cases and pragmatic capabilities for the warfighter. It explains why investing and maturing QIST matters for national security.

The quantum imperative: Why securing a quantum advantage matters

After years of general disinterest, U.S. leaders now recognize that developing, maturing, and fielding pragmatic and rugged QIST capabilities is important to U.S. national security interests on multiple fronts. Quantum capabilities could constitute a leap ahead to a new regime of competition, subverting adversary countermeasures, technologies, and strategies.[5] This is particularly important given that adversaries are aggressively seeking to deny traditional U.S. military advantages. Quantum sensors, for example, could offer accuracy, stability, sensitivity, and precision that far exceed those of classical technologies.[6] Quantum computers hold the promise to rapidly solve algorithms that classical computers cannot, including breaking the encryption that secures financial data and national security secrets.[7] These are clearly capabilities that U.S. adversaries could also exploit. That is why it is critical for the U.S. DOD to understand and shape the development of these capabilities for national security. The Congressional Research Service recognizes both sides of this coin and noted that as quantum technologies are integrated into military capabilities, "They could hold significant implications for the future of international security writ large."[8]

As an emerging field, it is not possible to fully anticipate all the potential use cases for QIST technologies. Consider the emergence of the first general-use digital computers as an analogy. Built in 1945, the electronic numerical integrator and computer (ENIAC) served the initial purpose of solving cumbersome mathematical equations and other limited problems, like ballistic trajectories, in laboratory settings.[9] Few computing experts of the time could have predicted how computer processing would evolve into ubiquitous, everyday use in smartphones, modeling and simulation, computer-generated graphics, or countless other applications. Today's leaders already realize that QIST may prove to have a similar transformative impact on the world—they simply lack clarity on the shape of that transformation.

As early as 2018, Congress passed the National Quantum Initiative (NQI) because they recognized that QIST was on the cusp of transitioning from primarily academic theory and experimentation to real-world applications. The intent of this legislation is to shepherd a "whole of government approach to ensure the continued leadership of the U.S. in QIS [quantum information science] and its technology applications."[10] This act implicitly acknowledged the importance of QIST to the security, economy, and global leadership of the United States. The legislation directed a National Quantum Coordination Office (NQCO) to develop a ten-year plan to accelerate QIST applications across multiple sectors.[11] NQCO activities and oversight include coordinating efforts among federal agencies, providing funding to basic research in universities and federal laboratories, developing the workforce, and establishing standards.[12] The NQCO also established the Quantum Economic Development Consortium (QED-C), a membership organization whose mission is to grow the commercial quantum industry and supply chain.[13] As proof that quantum's progress continues to be a specific point of interest for Congress, subsequent National Defense Authorization Acts and the 2022 CHIPS and Science Act buttressed U.S. government interest in and support for the development of QIST in the United States.[14]

These starter initiatives, however, may not be sufficient to establish and maintain a quantum advantage against China, Russia, and other global competitors. China is investing heavily in QIST R&D, and the nature of the Chinese model enables the Chinese Communist Party (CCP) to impose extreme focus on its own national QIST efforts.[15] But what does "quantum advantage" mean? Policymakers may be surprised to find that quantum scientists define "quantum supremacy," "quantum advantage," or "quantum primacy" in very narrow academic parameters: the ability of a quantum computer to solve a problem that no traditional computer could do.[16] This description might be useful for theoretical or experimental scientists, but it is not useful for a strategist or policymaker engaged in long-term competition against a peer adversary—supremacy, advantage, and primacy mean something very different to DOD entities when they are referring to military capabilities. Solving a specific computational problem is not the same as securing the ability to emerge victorious from an armed conflict. Senior leaders should be careful to ensure that they and their technologists are on the same page when they discuss securing and maintaining a quantum advantage.

A more useful working definition of "quantum advantage" for DOD would evaluate the comparative technological positions of the United States and adversaries like China with respect to their QIST efforts. This description may include the scientific research base that is often resident in universities and federal laboratories; the industrial base and skilled workforce capable of manufacturing both quantum and classical hardware; the intellectual workforce of quantum design, engineering, and programming; and the relative military value and threat assessment of fielded capabilities, as well as the readiness of warfighters to employ them. This comparative assessment offers a far more practical understanding of "quantum advantage" because it honors the global strategic nature of the competition. This definition, unlike the more academic one, also recognizes that quantum advantage is not a "zero-day" event but rather a marathon.

Working from this more relevant definition, senior defense leaders with a sufficient grasp of the science behind QIST will be better positioned to make informed assessments regarding quantum applications in the battlespace. Peer adversaries like China are now fielding capabilities that challenge many classical technologies that underpin U.S. military supremacy, such as GPS provided by undefended assets on orbit, and QIST has the potential to offer solutions to these emerging vulnerabilities. However, if leaders fall victim to the misconceptions, technological optimism, or breathless hype that often surrounds emerging technologies, they may fail to effectively resource the most value-added and high-potential QIST capabilities on a timeline to out-compete China. They may also fail to understand the strategic consequences of progressive and ongoing Chinese QIST demonstrations.

Why do senior leaders need a basic understanding of quantum science ?

Even for leaders with technical backgrounds, the confounding nature of quantum science makes it difficult to understand the technical premise, use case, or readiness of quantum-based capabilities. The principles, behaviors, and attributes of subatomic matter do not conform with our everyday experience of the world and how it works. For example, it is traditionally accepted that the world is made of particles. However, this "fact," that something as simple as particles exists and behaves according to predictable physical principles, is one that quantum sciences challenge. In quantum sciences, particles can sometimes exist as waves—or both simultaneously. The suggestion that advances in QIST mean the "known" physical properties of the universe could be manipulated is clearly attractive—and terrifying—to defense leaders and warfighters who often run up against the realities of physics—and depend on them. It is also clear how an exploration of such possibilities can quickly land in the realm of science fiction or operational impracticality. For example, quantum radar is theoretically sound, and its logic for detecting stealth aircraft appears compelling. Yet when the science behind quantum radar is placed in an operational context, this capability is impractical for actual use in combat. Defense leaders and policymakers may struggle to understand common quantum terminology, what it means, and how quantum theory and science translate into warfighter capability. Sorting science fact from science fiction demands that defense leaders increasingly possess a solid enough grasp of quantum science to intuitively and pragmatically ask the right questions and make sense of this new realm at a macro level. With a well-grounded basic understanding of QIST, they will be better equipped to evaluate the operational potential and readiness of QIST programs, both of which are crucial when making resource decisions and understanding broader strategic implications.

Defense leaders often depend on subject matter experts to guide their decision-making, but without basic knowledge of QIST, they will lack any ability to judge for themselves whether proposed projects may have real value to the warfighter. What works in the laboratory and may even technically work in the real world might not always be practical or useful for the warfighter. Senior leaders must have their own understanding to make informed requirements, resourcing, and programmatic decisions. This does not mean that they need to become quantum scientists or solve complex mathematical equations, but they should be sufficiently literate to ask the right questions, match the technology to high-value use cases, and identify key technological challenges. Unfortunately, the Defense Science Board's most recent assessment found that "there is a notable lack of rigorous analysis tying performance to mission specifications and/or novel capability."[17] In other words, more work is required to understand how the foundational principles of quantum sciences can address capability gaps and vulnerabilities for the warfighter.

The leadership perspective is crucial because scientists and engineers who are enthusiastic about transitioning QIST from the laboratory to the real world may likewise not fully understand the demands of the operational environment or how the quantum capability could or should be integrated with other systems. Technological optimism may lead program managers to overestimate the effectiveness of the proposed application or underestimate the quantum and classical challenges in maturing the tech into a combat capability. Innovators approach QIST from mathematical, scientific, and even theoretical vantages. Warfighters are needed to provide the operational perspective.

Understanding the basics of quantum science

Quantum technologies are not new, but recent advances in the field of quantum mechanics, material sciences, and other classical technologies have created the potential to use QIST in new ways. Long-established applications of quantum phenomena include atomic clocks, lasers, solid-state semiconductors, solar cells, LEDs, and charge-coupled devices (CCD) used for digital imaging and optical sensors, among others. These early breakthroughs exploited the quantum behaviors of technologies, but as National Institutes of Standards and Technology (NIST) physicist Ray Simmonds notes, these devices do not "control all of the quantum systems at the quantum level." Lasers, for example, exploit quantum principles to emit a very precise wavelength and focused beam but do not control individual photons.

Simmonds describes current advances in quantum sciences as "the second quantum revolution.... You're engineering the quantum mechanics itself to do something, not, 'Oh, I have a widget that has these special properties because of quantum mechanics.'"[18] In today's second quantum revolution, researchers apply advances in the underlying quantum sciences to deliberately isolate, control, and manipulate quantum particles to capitalize on quantum behavioral principles like superposition or entanglement to engineer radically new technologies.[19] A basic, conceptual level of understanding of these quantum principles and phenomena is critical for those making decisions about quantum investments for defense. At the very least, it is important so that senior leaders know what questions to ask to gauge the feasibility of quantum technologies and determine if there are use cases that make sense for warfighters.

What is "quantum"?

Classical or Newtonian physics describes the theories and mathematics that accurately describe and predict the larger physical world that we interact with daily. However, classical physics cannot explain the many strange and contradictory observations that scientists can measure at the subatomic level. One such observation involves the energy states of electron fields that surround an atom's nucleus and appear to jump in value between each orbital level. Classical physics cannot explain these distinct, or quantum, steps in energy state—hence, the nomenclature of quantum physics.[20] Although the subatomic world exhibits many other inexplicable behaviors and principles, "quantum" has come to broadly refer to any of these observable phenomena and the technologies that rely upon their science.[21] "Quantum" colloquially refers to the theories, science, and technologies encompassed by quantum physics.

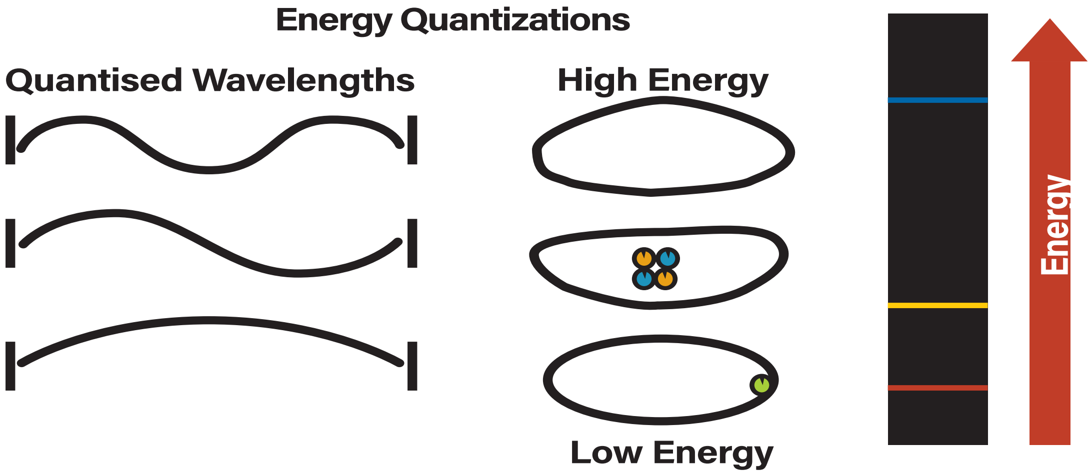


Figure 1: An early clue that subatomic behavior did not follow classical physics are the very tight frequencies of light emitted when electrons move from one orbital regime to another. Classical physics would have allowed any energy state, but experiments showed a specific "jump" of energy that correlated to specific wavelengths.

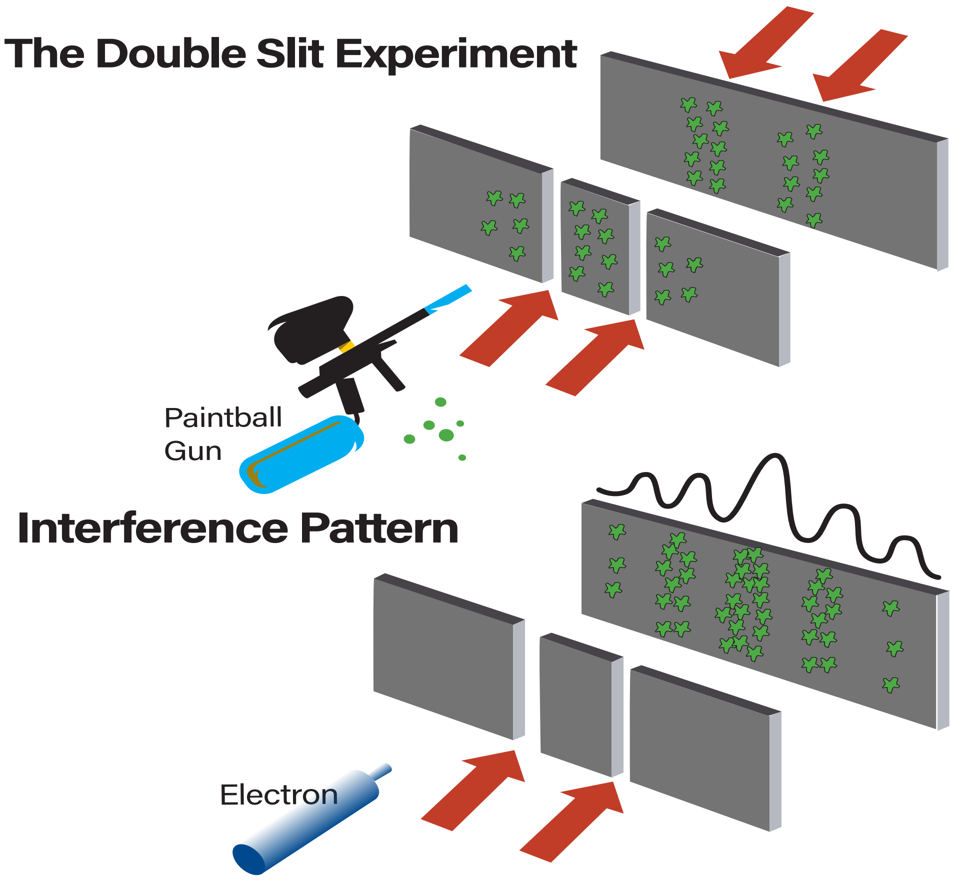
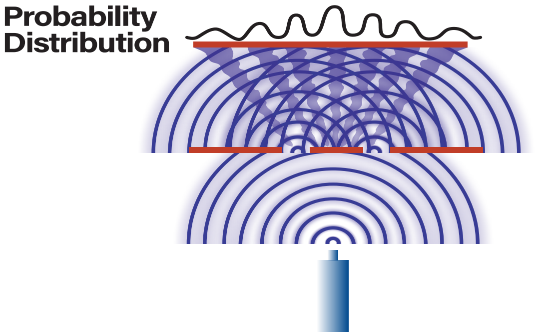


Figure 2: Wave-particle duality as illustrated by the double slit experiment. If quantum particles behaved like particles, then we would expect an impact pattern that mirrored the two slits—just like what would happen if paintballs were shot through two slits. Yet when electrons or photons pass through the double slit, scientists observe multiple lines of impact.

Image credits: Adapted from Dr. Dominic Walliman on YouTube: "The Domain of Science," by Dash Parham and Mitchell Institute.

Much of the strangeness of quantum physics is the consequence of **wave-particle duality**. While we think of matter and the atoms that make up our physical world as particles that resemble miniature golf balls, at the subatomic level, matter behaves more like a wave or ripple in a pond. Physicist Thomas Young first observed this behavior in his famous 1801 double-slit experiment, shining light through a filter that had two narrow slits.[22] He designed the experiment to test whether light was a wave or a particle. Instead of resulting in a pattern that mirrored the two slits, the single light source resulted in an interference pattern, just like a wave would have. Scientists realized that mathematically describing subatomic particles as waves resolved many of the inconsistencies at the subatomic level that classical physics could not explain. This double-slot experiment revealed that wave-like behavior applies to any subatomic particle: everything—not just light—acts like a wave and has a **wavefunction**, which is the mathematical equation that describes the wave.[23] The wavefunction describes the properties and probabilities of the quantum particle.



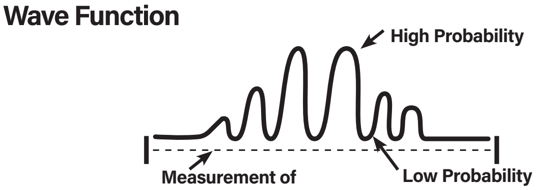


Figure 3: The double slit impact pattern is only explainable if sub-atomic particles behave like waves, not particles. This interference pattern matches what one would expect from ripples on a pond. In this experiment, the height, or amplitude, of the wave indicates the probability of where the particle is likely to be.

Figure 4: Wavefunctions are mathematical equations that are very effective in describing quantum's wave-like behavior, such as position (amplitude) and momentum (frequency or wavelength).

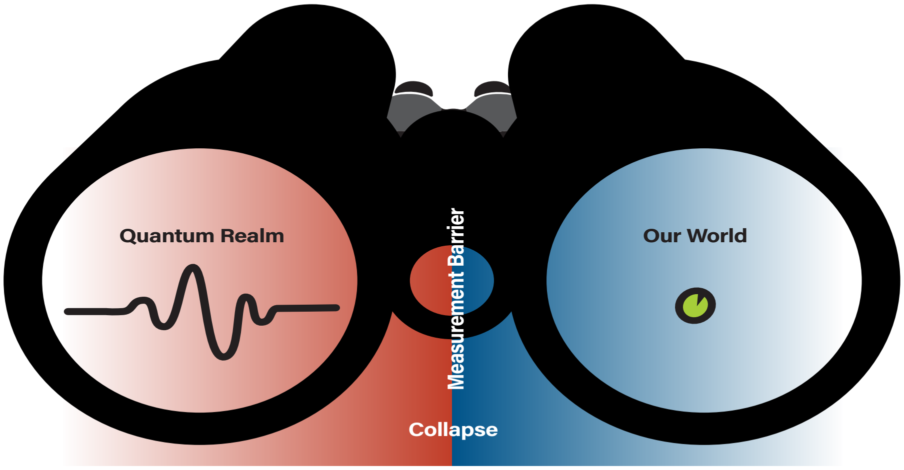


Figure 5: The wavefunction "collapses" into a discreet particle with specific characteristics when scientists seek to measure it. Special attributes, such as superposition or entanglement, are lost when the wave collapses into a particle. Scientists do not know why this happens and cannot explain it.

Image credits: Adapted from Dr. Dominic Walliman on YouTube: "The Domain of Science," by Dash Parham and Mitchell Institute.

While a good generalization of quantum physics is that subatomic matter behaves like waves, when physicists make direct measurements or observations of wavefunctions, they detect particles. **Physicists call this "collapsing" the wavefunction, meaning the quantum system ceases to exist in more than one state when it is measured**.[24] This wave-particle duality is a foundational principle of quantum physics: matter is simultaneously both a wave and a particle, and its state depends on how the waveform interacts with the larger physical world.[25] Wave-particle duality, the wavefunction, and wavefunction collapse all have profound consequences for how engineers can exploit the attributes of quantum science to create novel military capabilities.[26]

Wavefunctions are highly accurate in describing and explaining the subatomic world. The amplitude—the highs and lows of the wave—represent probabilities of the location of the particle. The frequency—how closely the waves are spaced—represents probabilities of where the particle is going (its momentum or vector).[27] In classical physics, an object has a well-defined and precisely knowable position and velocity. In quantum physics, the wavefunction is a "probability distribution in time and space."[28] A consequence of the wavefunction is that one can observe either the position of the particle or its trajectory, but not both. This inability to empirically know all the information about a subatomic particle is known as **Heisenberg's uncertainty principle**.[29]

The wavefunction is also a useful way to understand **superposition**. Superposition is perhaps most commonly understood through the "Schrodinger's cat" thought experiment—that the cat in the box is both dead and alive until one opens the lid to observe its deadness or aliveness.[30] It is important to emphasize that this is not simply a matter of the observer not knowing which state the cat is in until they open the box. The cat exists in both states simultaneously, and it is the act of observation that makes the cat dead or alive. Similarly, superposition is often described as allowing a quantum system or subatomic particle to simultaneously be in all possible states until it is measured–described

Heisenberg's Uncertainty Principle

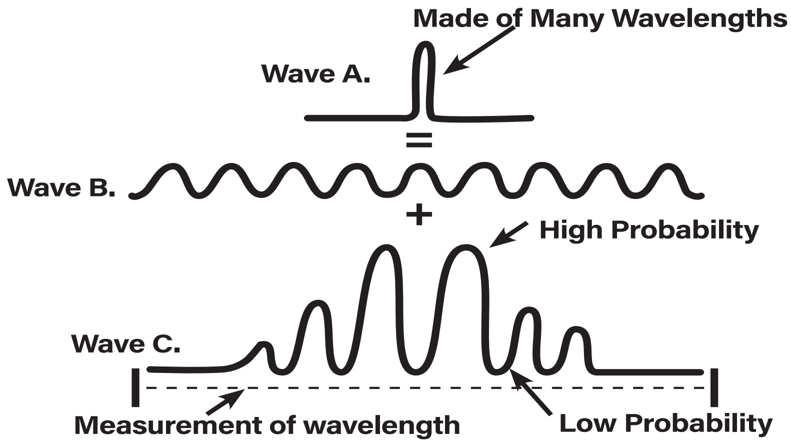


Figure 6: Because subatomic particles are also/simultaneously waves, it is impossible to fully know everything about their quantum behavior, such as momentum or position. In the wavefunction, amplitude can be understood as probability of position while wavelength, or frequency, provides information about its momentum. In wave A, one can have high confidence in the position of the particle but not its momentum. Wave B provides high quality information about the particle's momentum but not its position. Finally, wave C provides information on both position and momentum, but neither are very certain.

Image credits: Adapted from Dr. Dominic Walliman on YouTube: "The Domain of Science," by Dash Parham and Mitchell Institute.

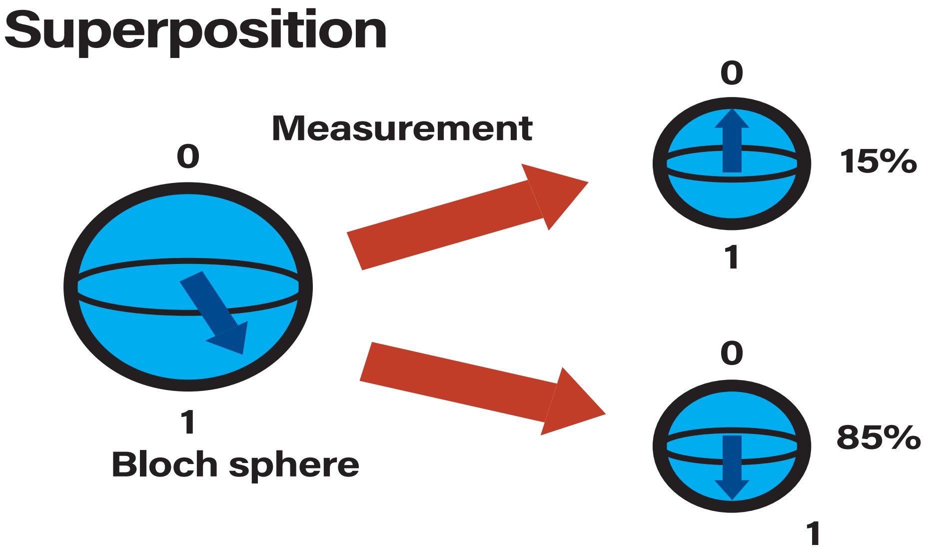


Figure 7: Although highly simplified, the 3-dimensional Bloch sphere is a useful way to visualize the different states and probabilities of the qubit. The arrow represents the probability of the wavefunction to be in a 0 and 1 state. In this example, the Bloch sphere is representing a superposition state that has a 15 percent chance of "0" and an 85 percent chance of "1" when it collapses. But just as wavefunctions are 3-dimensional, the arrow can point in any direction in the sphere. Moreover, this graphic is a snapshot in time—the arrow would change direction and rotation as a function of frequency and wavelength.

above as "collapsing" the wavefunction.[31] The wavefunction, however, tells us more about the probability of the quantum state.[32] When the wavefunction is measured, the superposition collapses into a classical state that has a definite value (even if the other properties of the particle are not knowable).[33] The ability to collapse the superposition into a classical state, or eigenstate, is a crucial piece of quantum computing.[34]

A consequence of uncertainty is that it is impossible to make an exact copy of a subatomic particle. This is called the **"no cloning"** principle.[35] In classical physics, the attributes of any object are measurable, and the more precise the measurements, the more precise the knowable information about the object's properties. But because the act of measuring collapses the wavefunction and changes the properties of

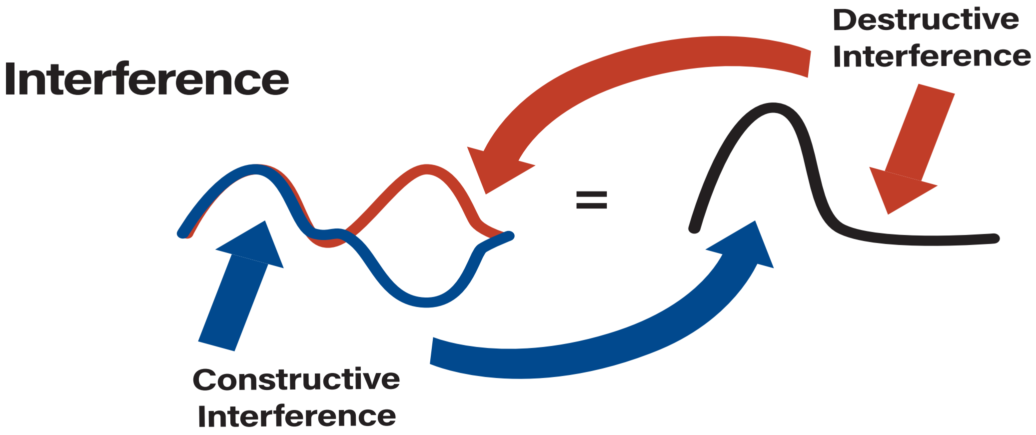


Figure 8: Quantum interaction is best characterized by adding their wavefunctions together. These interactions can be constructive or destructive, and change the frequency, slope, and amplitude of the total wavefunction. A familiar example of destructive interference are active noise-canceling headsets, which use opposing waveforms to null out external noise.

Image credits: Adapted from Dr. Dominic Walliman on YouTube: "The Domain of Science," by Dash Parham and Mitchell Institute.

the quantum particle, all the attributes of a subatomic particle cannot be wholly known or measured; ergo, a subatomic particle cannot be replicated.[36]

Interference is another quantum principle that results from the interaction of subatomic wavefunctions.[37] Unlike classical representations where atoms bounce off each other like billiards on a pool table, interference is best visualized as the wave properties of matter merging with each other to amplify, null, or otherwise alter the wave pattern.[38] This is similar to how ripples on a pond, waves in the ocean, or even soundwaves in noise-canceling headsets interact. Interference between quantum wavefunctions unites their characteristics and can change the amplitude, frequency, or other properties of the combined wavefunction.[39]

Interference can also entangle particles. **Entanglement** is a phenomenon where quantum particles are generated, interact, or share an external stimulus that creates a perfect correlation between them.[40] This does not necessarily mean that the particles are now identical. Instead, this means that a single, combined wavefunction now describes the entangled particles as an integrated system—a common, unified quantum state where the properties of one particle are dependent on the other.[41] Entanglement causes particles to lose their individuality and act as a coherent entity or system.[42] A commonly used example is photons: if a researcher entangles two photons such that the unified wavefunction has a spin of zero and then measures one as having a clockwise spin, the other photon would have a counterclockwise spin. The opposing spins would cancel each other out, netting an effective spin of zero for the wavefunction.[43]

This correlation remains true even if the entangled particles are separated by large physical distances, a property known as **nonlocality**. Nonlocality describes the principle that entangled particles can be influenced or affected by forces that are not within their immediate or local environment. Entangled particles can be widely separated—even by billions of miles—and still retain their entangled relationship. Physicists have tested nonlocality by observing previously entangled and then separated photons, and they have consistently observed that the entangled photons are correlated.[44] But because measuring entangled particles collapses their wavefunction, it also destroys the entanglement.

Albert Einstein rejected nonlocality to his death, complaining that it was "spooky action at a distance." How could entangled particles instantaneously "know" and respond to the state of the other, such that they remained coherent as a system no matter how far apart they were? To Einstein, this correlation threatened to violate the speed of light.[45] Yet, nonlocality has been consistently demonstrated in a dynamic that physicists describe as **quantum teleportation**.[46] Entangled particles, because they are part of a coherent system, appear to instantaneously transfer quantum information from one particle to the other nonlocal particle, and scientists call this quantum teleportation.[47] While the seemingly instantaneous nature of exchange remains a mystery, in practical application, teleportation still requires classical information to be transmitted across classical networks to reconstruct the message content.[48] For human communication purposes, quantum teleportation does not violate the speed limit of light.

Why do these quantum principles matter?

Scientists and engineers can now deliberately control matter at the quantum level to apply these principles to solve problems in the larger, physical world. Unlike the first quantum revolution, which used quantum principles to create classical technologies like lasers and MRI machines, the ability to deliberately manipulate subatomic systems opens exciting possibilities for advanced military applications. For example, quantum positioning, navigation, and timing (PNT) could sidestep adversary counterspace strategies by providing alternatives to the GPS constellation. Quantum RF could dramatically enhance passive sensing, and quantum sensing could provide much better detection than classical capabilities.[49]

The sensitivity of quantum systems, however, offers both benefits and challenges. Quantum matter can enable much higher levels of detection and precision than classical technologies, but its states are fragile and extremely susceptible to unwanted inputs from the environment and other external stimuli.[50] These environmental influences could be from magnetic or electric fields, radiation, heat, or even "cross-talk" between the quantum systems.[51] This noise can induce **decoherence** of the quantum system, disrupting its state and interfering with and entangling it in ways that cause degradation and errors.[52] Once the quantum particle decoheres, information encoded in the particle is corrupted and induces error in the quantum system.

To build effective quantum technologies such as computers, sensors, or communication systems, engineers and scientists must be able to create a quantum system that has the ability to control entanglement and superposition in the face of noise and unwanted external interference and then not degrade or diverge over time.[53] The ability to maintain long-term coherence or control the quantum system free of unwanted interference will be crucial to fielding pragmatic and rugged military capabilities. **Defense leaders will, therefore, need to press scientists on the coherence of quantum solutions.**

Understanding the different ways to access and control quantum properties

All quantum systems are built on quantum bits, or qubits, and how technologists build qubits can vary widely—and so can qubit performance. Quantum states are very sensitive, a property that makes qubits very useful but also very fragile. **As technologists continue to evolve qubit design, senior leaders should continually press them on the ruggedness of qubits for operational employment.**

While quantum principles and properties are universal, the physical methods and hardware, or **modalities**, that physicists use to isolate, control, and measure quantum matter are not. Scientists use various modalities to build qubits and access quantum properties. Some modalities use cryostats, a system used to maintain very low temperatures, to get their qubits to near absolute zero, while others use lasers to control and manage their atomic qubits. There is no single best modality or qubit type for all applications, and the modality is often driven by the research preference of the scientists or the business and technical goals of the company or organization. One modality may be more effective at large-scale computing, while another modality may be better at sensing. Each modality has different strengths and challenges and should be matched to the technological use case.

The choice of modality impacts technology design—the classical hardware and software it depends on—and the attributes of the qubits themselves. The quantum modality of the technology will impact the operational performance of the capability with real combat outcomes. **Policymakers should strive to understand the benefits and drawbacks of each modality and its qubits so that they may make informed decisions regarding how to best match modalities to their use cases.**

What is a qubit, anyways?

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 computing, bits were electrical transistors that were either powered on (a state of 1) or powered off (a state of 0).[54] The difference, though, is that a qubit can be in a state of superposition, a combination state between 1 and 0.

At the physical level—not an abstract mathematical or conceptual level—the value of the qubit is characterized by attributes like spin up or down or the vertical or horizontal spin of the particle.[55] Physical qubits can be composed of many different types of particles: electrons, ions, atoms, or photons. The state or value of the qubit, as described, is not known until it is measured. It is neither 1 nor 0; it is a 1 and 0. More specifically, the 1 or 0 state of the qubit is a probability—a statistical likelihood somewhere between a 1 and a 0 that enables the qubit to be both. The superposition of a qubit is best visualized as a Bloch Sphere.

A Bloch Sphere is a three-dimensional sphere with a vector whose tail is at the center of the sphere. The value of the qubit is represented by where the head of the vector's arrow is pointing in the sphere. If the arrow is pointing directly up, it's in the 1 state, and if it is purely pointing down, it is in the 0 state. Any direction other than purely up or purely down is a superposition, which is a probability of the state the qubit will collapse to when measured. For example, purely up or purely down is also a probability—a "100 percent" probability.[56] Phase is represented by the "east" and "west" hemispheres in the Bloch Sphere.[57] Measuring the qubit collapses its superposition into a classical state of 1 or 0, and the probability of either outcome is determined by the position of the arrow.[58]

Qubit fragility

A major challenge for any quantum system is that because of their inherent fragility, qubits are prone to error. The same quantum principles and sensitivity that make qubits so useful for computation, sensing, and other applications also make them vulnerable to noise from the environment, such as radiation, heat, impacts from other particles, or even the machine's control systems.[59] **Noise** is any kind of interference with the qubit's behavior and attributes, and it can induce decoherence and other errors in the quantum system, as well as unwanted interference and entanglement with the system's qubits. Qubits themselves are "noisy," interfering or entangling with each other in a phenomenon called **cross-talk**.[60] Thus, the more qubits in a system, the noisier the system. Moreover, depending on the modality, some qubits are more susceptible to errors than other quantum modalities. All of this can collapse the qubit, induce unintended entanglement, or create unintentional wavefunction interference, thereby threatening the integrity of the information of the qubit or the quantum system's process.

Applying logical qubits helps control for these errors in an effort to create fault-tolerant quantum systems. **A logical qubit is one or a grouping of qubits with a longer coherence that corrects for the faults induced by noise**. Rather than shielding and striving for perfect qubits, a fault-tolerant system seeks to implement a sort of quality control to compensate for qubit errors. There are different ways of doing this kind of correction, but one of the most common means of doing this is to entangle many different qubits together to achieve one "noise-free" or "idealized" logical qubit.[61] Other approaches use parallel qubits to perform a range of tasks, such as spotting and correcting errors as they occur or simply executing the task thousands

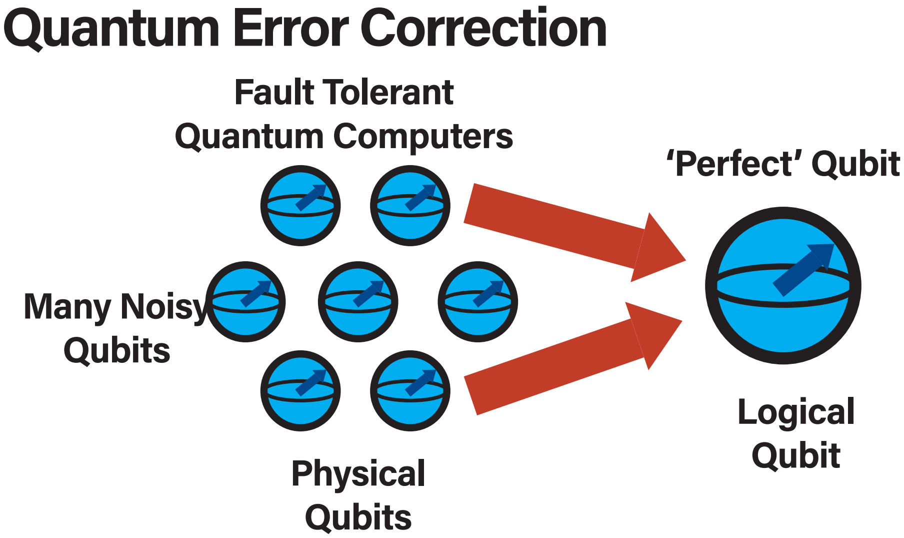


Figure 9: Qubits are the quantum equivalent of a traditional "byte" of binary information. But because they are easily influenced by noise, cross-talk, or can randomly decohere and distort or even lose information, qubits themselves can induce errors in quantum systems. There are several ways to counter the errors induced by these "noisy" systems: use other qubits to monitor the algorithm to error correct real-time, run the algorithm repeatedly to statistically correct for errors, or use many qubits to simultaneously process the algorithm. The net effect is the same: Fault tolerant quantum systems require an overhead, or larger number of actual qubits that correct for noise and are one of the most common approaches used by technologists. This corrected equivalent is called a "logical qubit."

Image credits: Adapted from Dr. Dominic Walliman on YouTube: "The Domain of Science," by Dash Parham and Mitchell Institute.

of times and statistically determining the most probable solution.[62] The need to correct for these errors defines the current era of "noisy intermediate-scale quantum" (NISQ) systems.[63] Until technologists are able to build clean, noise-free quantum systems, the scale of quantum computers may be limited. To realize the full potential of quantum computing and other QIST applications, scientists will need to develop fault-tolerant systems that can reliably solve large-scale computations without the high overhead of redundant, logical qubits.[64]

What this means for policymakers is that they should ask programs and vendors about the overhead of logical qubits, especially when it comes to computational systems. Not all qubits are equal, and not all error correction techniques require the same volume of extra qubits. While scientists are still working through how to best and most efficiently correct for qubit errors, what is relevant is that a basic qubit is not analogous to a classical bit, and this informs how defense leaders should understand claims about quantum systems, especially quantum computers. Additionally, there are many different types of qubits that are dependent on the modality used for the quantum system.[65]

Understanding quantum modalities

Quantum modality refers to the type of particle used to produce the qubit and the hardware approach used to control and manipulate the qubit. Qubits can be classified based on the primary particles scientists use to build them: electrons, atoms, and photons.[66] Different companies and quantum teams use different hardware and control modalities to isolate, control, and manipulate their chosen qubit.[67]

As each modality type uses different quantum particles and manipulates them in different ways, a consequence is that each modality will have different qubit performance outcomes. The speed and fidelity of quantum logic gates are one example. **Logic gates** are the physical controls that software engineers use to execute algorithms, computations, and programs. In the classical, binary world, this is literally opening and closing the electrical circuit (the "gate") based on the gate logic.[68] Quantum computers, the primary users of gates in quantum systems, need specialized types of gates that accurately manipulate the qubits without distorting their desired state or collapsing their superposition. However, gates are a physical means of controlling the logic of the information contained in the qubit, so each modality performs differently when it comes to attributes like gate speed or fidelity. Performance metrics of a modality should ultimately be judged by its application and practicality. For example, choosing a modality based on its gate speed may not be a relevant consideration for a quantum inertial navigation system. Any inertial navigation system measures the forces of acceleration to determine changes from an original, known position. Quantum inertial navigation exploits the sensitivity of quantum particles to measure these acceleration forces on atoms and does not use logic gates. If Department of the Air Force leaders do not understand the nuances of how to assess the attributes of modalities against use cases, they may risk pursuing developmental programs that do not optimize the modality for the needed capability.

Aside from performance and effects, external considerations can be equally important to senior leaders when it comes to quantum modalities. For example, superconducting chips may be easy to fabricate using modern and well-established manufacturing techniques, but their need for extreme cryostat refrigeration to operate may be impractical or impossible to accommodate on the front lines and limit this modality's defense applications. Conversely, certain technical approaches may have unique benefits in specific battlefield applications that cannot be matched by other modalities. The neutral atom modality, for example, may prove extremely flexible across use cases that range from computation to timing and sensing. To fully harvest the potential of QIST, policymakers should be prepared to invest in several different modalities because different approaches may prove more advantageous for various applications. When it comes to QIST applications such as quantum computers, sensing, or communication, there is no single "best" approach.[69]

Senior leaders must understand that each quantum modality has its own unique advantages and challenges, which may define their potential operational use case and subsequent technical development.[70] **As with any technical design, understanding the tradeoffs between capability, cost, complexity, size, and operational utility of the quantum modalities is critical to making decisions about investment and procurement. Policymakers should probe these considerations to better understand the strengths and limitations of each so they may focus research and development efforts on the best applications for the warfighter.**

Types of modalities

Electron-based modalities. These approaches use electrons as the basis of their qubits. 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 certain threshold temperatures.[71] At temperatures colder than outer space, these superconducting materials lose all electrical resistance, and entangled electron pairs, called Cooper pairs, flow freely and indefinitely around the closed loop.[72] This circuit is the qubit, and its quantum state (wavefunction) can be manipulated by magnetic flux, microwave oscillators (charge), or Josephson gates (flux).[73] These three basic methods of chip design, electron control, and measurement define the superconducting qubit types: the charge qubit, the phase qubit, and the flux qubit.[74] Designers pursue a specific design and type based on performance goals, such as minimizing noise or cross-talk, increasing gate speed, or extending coherence.[75] Superconducting qubits are used primarily in quantum computers and are rarely found in other quantum applications.

Superconducting chips are an attractive modality because they are similar to classical chips and use similar fabrication methods.[76] Moreover, the circuit logic of these qubits is like that of classical processors, creating a familiar analog for quantum chip designers and programmers. Because of this, they are a better-understood modality, and there is significant cross-over from conventional chip design. Moreover, superconducting chips have high gate speeds for fast computations, high connectivity, and excellent qubit fidelity.

This does not mean that superconducting qubits are the ideal modality—electrons are very reactive and easily decohere from charge, magnetic flux, or photon and other quasiparticle interactions.[77] Consequently, superconducting chips suffer from short coherence times for calculations.[78] As manufacturing techniques continue to improve, the error rates and coherence durations will likely improve, too.

Perhaps the biggest drawback of this modality is the sizeable infrastructure needed. Driven by its huge cryogenic power demands and space requirements, these computers are large, heavy, and immobile. For example, IBM's 2019 Quantum One system, a 20-qubit computer, stands roughly 9' x 9' x 9'.[79] In any of the cryostat-dependent modalities, it is not the qubits themselves that drive energy requirements—the dilution refrigerator and the control systems are massive and power-hungry.[80] The larger the quantum volume, the larger the footprint and the higher the energy demands are for the support system.[81] This may limit the potential for these quantum systems to scale or deploy in a battlespace.

Quantum dots, also known as silicon spin, are another electron-based qubit. The dot itself is made of a few thousand atoms of a semiconductor, often silicon, and although the dot is thousands of atoms, a single trapped electron comprises the qubit.[82] There are two types of quantum dot qubits: the spin and the charge qubit.[83] Similar to superconducting circuits in their infrastructure requirements and chip manufacturing, their major difference is that instead of flowing electrons

Modality Type	Benefits	Challenges
Superconducting Chips	Strong gate fidelity Can leverage existing microchip fabrication Small form/fit of chips similar to current chip High gate speeds = faster processing times Circuit logic similar to 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

in a circuit, quantum dots trap electrons on the chip in electro-static wells between semiconductors that look like teeth on a comb. The qubit's charge or spin is manipulated by electrical or magnetic fields, and oscillators can be used to entangle electrons.[84]

Quantum dot or silicon spin modalities share many of the same advantages and drawbacks as superconducting chips. Like superconducting chips, quantum dots can leverage the fabrication expertise and facilities of traditional chip manufacturing. Similarities in the construction enable fast gate speeds and high fidelity of the qubit through operations. However, quantum dots have short coherence times and struggle with cross-talk. At the same time, the nature of the chip design isolates the qubits from each other, leading to low connectivity and limited entanglement volumes. Quantum dots also share the same cryogenic infrastructure requirements as superconducting qubits—a major drawback for many military applications.

Atom-based modalities. The two major atom-based modalities are neutral—or cold—atom and trapped ion. Both modalities use lasers as key supporting technologies. Consequently, they do not require the cryostat or dilution refrigeration infrastructure of electron-based modalities. Moreover, atom-based modalities are far more flexible, opening potential use cases and applications that expand well beyond computation.

The **neutral atom, or cold atom**, approach uses lasers to trap single atoms into a geometric, optical lattice. Neutral atom approaches typically use non-alkaline earth elements such as strontium or rubidium as their atom base.[85] These elements exist in a solid state at room temperature, so first, they must be heated into a gaseous state to create an elemental vapor. This elemental vapor goes through multiple stages of cooling using lasers that de-excite the individual atoms to a temperature near absolute zero without allowing them to condense into a solid state.[86] After the atoms have reached this ground state, another multi-focused laser is aimed into the vacuum cell to create an optical lattice. The interference pattern of the lasers creates three-dimensional "highs" and "lows" of energy hills and wells. Manipulating the aim of the lasers shapes the interference pattern and can act like a set of optical tweezers, placing each individual atom in any configuration desired inside the optical lattice.[87] The resulting matrix or desired geometry of individual atoms remains neutral (not ionized) and defect-free.[88] Lasers are used to excite and entangle atoms as well as apply gates to enable digital computation.

The neutral atom approach has an impressive set of advantages and is extremely versatile. Neutral atoms offer a stable, identical, and consistent basis for qubits. They also have strong connectivity and very long coherence times—as long as five seconds.[89] For comparison, superconducting qubit coherence times are less than .2 milliseconds.[90] Moreover, neutral atom devices do not require the massive dilution refrigerators of electron-based modalities. The use of lasers to control the atoms and apply logic gates means that bulky wires are not necessary to connect qubits, and this enhances scalability in two and even three dimensions.[91] Neutral atom qubits scale easily and are very controllable and measurable. Because of this, neutral atoms can be used across a wide variety of applications, from annealing and universal computation to quantum simulation, timing, sensing, and radio frequency applications.[92]

However, the neutral atom modality comes with its own challenges. Gate fidelity and gate speeds are low for computation. This means that the function of the gate may not be accurately executed by the qubit, and these logical processes take longer than other modalities.[93] The neutral atom modality shows perhaps the most significant promise for a wide variety of applications, but defense needs will require further miniaturization of lasers, improvement in the precision of laser alignment, the miniaturization of ultra-high vacuum cells, and improvements in photonics.[94]

Trapped ion devices, like neutral atoms, rely on elemental vapor inside ultra-high vacuum cells.[95] An elemental vapor is created inside an ultra-high vacuum cell, and the atoms are then stripped of an electron by a laser. The resulting positive charge allows the atoms to be trapped and levitated in an electromagnetic field, where each can then be manipulated and measured.[96] Like the neutral atom modality, trapped ion devices use lasers to entangle atoms and perform gate functions, either simultaneously on multiple stationary qubits through careful use of the laser beam or by moving the ions next to each other for adjacent operations.[97]

Because of the similarities between these atom-based modalities, trapped ion devices share many of the same advantages of consistency in the qubits and very long coherence times without the burden of dilution refrigerators or other cryostat infrastructure. They also share many challenges, like slower gate—and, therefore, processing—times and the need to miniaturize and improve laser technologies. Unlike neutral atoms, however, trapped ions have extremely high gate fidelities, but the nature of how the ions, which can become unwieldy when massed, are trapped in free space may restrict their computational scalability.[98]

Photonic Qubit. Modalities based on photons, such as **quantum optical circuits**, manipulate the polarization or spin of individual photons—chargeless, massless particles of light—to encode information in the photonic qubit.[99] Photonic qubits, in other words, are photons deliberately encoded with information or entangled with other photons and can convey across fiberoptics as "flying qubits" or even travel freely in laser light beams. While photons are already used in many digital information technology applications conveying information through pulses of light, photonic qubits are rapidly emerging as a stand-alone modality, and they are also critical enablers of other modalities. Because flying qubits can physically travel from one place to another without decohering, they are critical to creating quantum networks, communication, and scaling quantum computers.

Modality Type	Benefits	Challenges
Neutral Atom	Application versatility 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	Application versatility 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 Trap design may restrict scalability

There are different ways to create photonic qubits, and quantum scientists characterize those methods as either "probabilistic" or "on-demand." Technologists most commonly generate probabilistic photonic qubits by pulsing a laser at a crystal to excite its atoms. This causes the atoms' electrons, which soak up the laser energy, to leap to a higher orbit—or energy state. When an electron's energy state decays and it returns to its previous orbit, it releases a photon—this occurs because of the law of conservation of energy in classical physics. But determining which atom, when, how many, the direction of the photon's travel or its spin, or other properties are inherently probabilistic.[100]

Methods for reliably generating "on-demand" photons—creating photons when desired—are still maturing, and these include manipulating quantum dots, lasers, trapped ions, or even semiconductors.[101] By tightly controlling the environment and the state of the donor atom, physicists can create a directional stream of photons.[102] The challenge, however, is reliably creating a high volume of high-quality photons that are identical, which, for quantum purposes, simply means indistinguishable from each other.[103] Identical photons are important to establish a baseline state from which the photon can be manipulated as a qubit. To bring each photon to a known baseline, scientists must filter photons through a waveguide or use tunable beam couplers and optical phase shifters on a photonic chip to adjust the photons to share standardized characteristics.[104] This step is crucial because the more standardized the photons, the fewer errors the system experiences.

The advantages of photonic qubits are that they have very high gate speeds and fidelity when used for computation. Moreover, photonic quantum chips can leverage existing technologies for design and manufacturing. These integrated optical circuits are similar to traditional semiconducting chips but flow photons instead of electrons through the chip.[105] As discussed previously, photons are the only physically mobile qubit modality that uses well-understood transmission means like fiberoptics or free space. Moreover, photonic qubit applications do not rely upon cryogenics and their associated power and infrastructure demands or specialized vacuum cells.

However, photons can be difficult to work with as qubits. Because photons have no mass, they can be difficult to control, and these systems can be subject to photon loss. Photons, which have no electrical charge, do not naturally interact, making entanglement or manipulating the qubit's quantum properties challenging.[106] One area where this can prove problematic is computation because the photons tend to be impervious to logic gate functions, meaning, in a sense, that they ignore or don't respond to the gate functions.[107]

Modality Type	Benefits	Challenges
Photonic	Application versatility Promising qubit fidelity Long coherence times Leverages microchip fabrication technologies Room temperature Often used in conjunction with atom-based modalities Can 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

Quantum modalities are key to understanding the quantum industrial base

The basics of quantum science and how engineers access, control, and manipulate quantum particles may seem unnecessary for senior leaders to understand, but these are the foundations of all QIST capabilities. Quantum companies are often formed around the founder's preference for or belief in one modality over another, and that modality choice enables or constrains possible applications. A QIST company's modality, design, and engineering have a direct impact on the quality of its qubits and ability to manipulate quantum particles and behavior. A company based on superconducting chips, for example, is unlikely to be able to develop a sensor appropriate to integrate on a fighter aircraft due to the cryogenic, power, and space requirements. Similar to how engine, sensor, and airframe makers are important to the aviation industry, each modality is an important component of the quantum industrial base.

A working knowledge of quantum science, its modalities, and how these come together to impact operational use cases is essential for any competent Department of Defense or Air Force leader, just like understanding the basics of mission equipment, production, and operational concepts. This knowledge is even more important given that today's senior leaders bear the responsibility for establishing and cultivating the quantum defense industrial base on which our nation will depend, as well as understanding the state of quantum competition with China. Department of Defense leaders either lay an effective foundation for future progress now or risk falling behind. This is a contest akin to a long-distance marathon, where steady progress is the key to victory, and a last-minute sprint will prove insufficient.

China's efforts to secure a quantum advantage

Based on the near-peer threats the United States faces today, fielding QIST capabilities is imperative for its national security enterprise. The DOD is not alone in recognizing the importance of this promising new technological advancement and finds itself in a race with global competitors, especially China. Experts estimate that China has invested upward of $15 billion across all of its QIST research and development efforts to date, a figure that far outpaces other countries, including the United States.[108] China now holds twice as many quantum patents as the United States and is aggressively pursuing QIST, which could have military applications.[109]

To this point, China launched its Quantum Experiments at Space Scale (QUESS) Micius satellite in 2016. Micius represents a dramatic milestone across years of effort by the Chinese Academy of Sciences (CAS) to harness the potential of QIST.[110] Initiated in 2011, QUESS sought to tackle the many difficult problems of quantum communication, including a new kind of encryption protocol. The 2016 Micius launch demonstrated China's ability to deploy quantum key distribution (QKD), a form of quantum-based encryption, between Beijing and a ground station in western China. The CAS team also used Micius to perform other experiments notable for the distances involved, and in 2017, they conducted the "world's first quantum-encrypted virtual teleconference."[111] This quantum communication, conducted with the Austrian Institute for Quantum Optics and Quantum Information (IQOQI), bridged a distance of over 4,600 miles. CAS has since continued to develop and demonstrate novel experiments designed to further secure quantum communications across "untrusted" nodes.[112]

While the National Security Agency (NSA) discourages U.S. entities from using QKD for encryption, China's ability to successfully execute the technological requirements of QKD at scale demonstrates its ability to produce and encode on-demand photonic qubits, maintain signal strength (avoid meaningful qubit loss) across thousands of miles using both free-space and fiberoptic transmission means, and develop secure and accurate quantum repeater stations.[113] Today, this quantum network includes two quantum satellites and 700 fiberoptic cables.[114] The Chinese QIST community can continue to use and develop this network; it serves as a foundational infrastructure to discover, understand, and solve the problems that become clear only once a capability moves out of the laboratory and into the real world. The United States does not currently have a similar architecture, and this is one soft measure of how China is winning the QIST race. Dr. Nicolas Gisin, a physicist at the University of Geneva, echoed the sentiment of many scientists in the field when he stated that "China has taken the leadership in quantum communication."[115] The ability to field these kinds of encryption and communication capabilities has clear use cases for military command and control operations.

However, the QUESS program is just one of many lines of effort the CCP is pursuing, and communications and networking are not the only areas where China has demonstrated substantial accomplishments that have been validated by the international scientific community. China has and continues to make significant strides in quantum computation. In 2021, the University of Science and Technology of China (USTC) revealed an advanced superconducting computer named the Zuchongzhi 2, after a famous Chinese historical mathematician and inventor, which utilized 56 qubits out of a total of 66.[116] What was remarkable was that the Zuchongzhi 2 "cracked a problem three times tougher" than what Google's Sycamore computer could solve.[117] Google's Sycamore computer is a 53-qubit superconducting computer that marked the first point of "quantum supremacy" in 2019.[118] However, the same year the Zuchonzhi 2 out-performed the Sycamore, the Chinese also demonstrated Jiuzhang 2, a photonic qubit computer whose computational speed and power far exceeds the Sycamore computer by factors thought to be in the billions—at least in highly controlled laboratory settings, for the time being.[119]

Aside from the construction of prototype quantum computers, Chinese researchers have been developing techniques to solve fundamental quantum challenges, such as error correction. Disconcertingly, a late 2022 paper by Chinese researchers from prominent universities also proposes a method of breaking standard RSA encryption with a 372-qubit computer.[120] RSA decryption, which could be used for a "harvest now, decrypt later" intelligence strategy, was previously estimated to require hundreds of thousands of qubits. While the paper is controversial in the scientific community and has not yet passed peer review, the research exemplifies China's steady advance toward cryptologic vulnerability.[121]

China has made other quantum claims that warrant scrutiny. Public announcements regarding quantum radar, for example, have met with skepticism from international scientists. Quantum radar sends out one particle of an entangled pair, keeping the other in storage. If the state of the stored particle changes, it represents a positive detection of a target. China has openly messaged its quantum radar as a jam-resistant counter-stealth capability, even marketing a prototype by the China Electronics Technology Group Corporation at the 2018 Zhuhai airshow.[122] A more recent 2021 paper from Tsinghua University claimed an improved quantum radar design that increased the probability of detection of a stealth object from 10 percent to 95 percent.[123] Other scientists, however, remain skeptical of all these claims.[124] The idea behind a quantum radar is that a photon changes when it bounces off a stealth aircraft and, therefore, changes the stored partner photon. But there are several issues with this; quantum storage is still early in development, you cannot monitor the status of the stored photon for change without collapsing it, and it would be very difficult to build a useful and accurate tracking solution. Quantum radar just does not provide the fidelity needed to justify the pursuit. French physicist Fabrice Boust's comments are fairly representative: "I am convinced that when they announced their quantum radar it was not working… but they knew they would get a reaction."[125] While the idea behind quantum radar is alluring, it is highly unlikely to mature into a pragmatic or relevant capability.[126]

Even if RSA decryption and quantum radar are primarily CCP propaganda, China has no intention of being left behind in quantum science or technologies.[127] In 2008, China established the "Thousand Talents Plan," a government-led program to recruit and employ foreign scientific researchers in Chinese industry and academia.[128] According to a U.S. Senate Committee report, this is just one of over 200 CCP talent recruitment programs to cultivate and accelerate domestic Chinese scientific innovation.[129] Talent recruitment programs go well beyond job postings: documented activities include conducting undisclosed scientific collaborations, obscuring Chinese institutional affiliations, academic and economic espionage, stealing intellectual property and technical data, and facilitating clandestine relationships with the People's Liberation Army (PLA).[130]

China's 14th Five Year Special Plan for Science and Technology Military-Civil Fusion, its newest strategic-economic plan to coordinate and prioritize efforts across the People's Republic of China, specifically highlights QIST, among other technologies such as artificial intelligence and machine learning, as a national imperative.[131] This accounts in part for the Chinese government's investment of an estimated $15.3 billion in quantum research to date.[132] Although there is some debate regarding the veracity of these financial assertions, if accurate, this would mean that the CCP has invested more than double the amount the European Union ($8.4 billion) and triple the amount the U.S. government ($3.7 billion) has in quantum basic and applied research.[133] Even at the most conservative estimates of a $4 billion investment to date, China is still outpacing U.S. government investment.[134]

By many measures, this aggressive approach is working for China.[135] The combination of "talent recruitment," centralized direction, and heavy and focused government funding has catalyzed China's quantum academic community and industry.[136] Roughly 52 percent of all QIST-related patents belong to Chinese researchers or companies, and China has twelve dedicated quantum technology research institutions.[137] Interestingly, China has around five QIST organizations, encompassing startup companies, incumbents, government laboratories, and universities, which seems anemic when compared to roughly 200 in the United States. However, this also means that funding is more concentrated, and activities are more focused in China than in the United States.[138]

The pace of QIST advancement is staggering, resembling a technological game of leapfrog between companies and nations.[139] China's experimental successes are clear evidence that it is making significant progress in developing its quantum technologies. These experiments also represent practical military applications, even if they are not yet fieldable. Their continued support and development are clear indicators that the CCP, and the PLA by proxy, are committed to solving the difficult problems of QIST and maturing the technologies needed for quantum capabilities to be useful to their warfighters. Secretary of the Air Force Frank Kendall acknowledged, "It is quite clear to me that we are in a race for technological superiority with China as far as conventional warfighting is concerned."[140] The director of the China Aerospace Studies Institute concurred, warning that hypersonics and quantum computing stand as "niche fields" where China is rapidly closing the gap.[141] Booz Allen Hamilton's head of Strategic Cyber Threat even assessed that China may be on track to surpass the United States.[142] No one can afford to rest on their laurels. As previously mentioned, this would be like the U.S. failing to innovate and lead in the field of microelectronics in the 1960s and 1970s—a foundational era that shaped everything for the United States and the broader world across the ensuing decades. America either commits to leading once again, or it risks ceding its technological edge along with the ability to set the broader QIST employment state of play for decades into the future. This would portend severe economic penalties and could prove disastrous from a national security vantage.

Conclusion

For the warfighter, there is no benefit to pursuing quantum science for science's sake. Clearly, the technology has to be developed and operationalized to prove useful. What matters in the battlespace is how these technologies can solve critical capability gaps and provide operational advantages in ways that facilitate successful and safe mission accomplishment. A requirements pull on research and development efforts, the scaling of manufacturing facilities, the production of a program of record, and capability integration are key to securing a quantum advantage—but the first step is for senior leaders to establish a solid and pragmatic understanding of the basics of quantum science. This foundation will empower decision-makers to sort through the hype, ask the right questions, realize their position in the global QIST competition, understand the threats, and focus their resources on the best modalities for operational applications.

Key takeaways for senior decision-makers

1. **A sound understanding of the basics of quantum science is crucial to empower U.S. defense leaders to evaluate proposed QIST applications.** This does not mean that they need to become quantum scientists or solve complex mathematical equations, but they should be sufficiently literate to ask the right questions, match the technology to high-value use cases, and identify key technological challenges. Understanding the principles of entanglement, interference, non-locality, teleportation, no-cloning, and so forth may seem highly esoteric, but it is vital to ensure that the discussions surrounding QIST programs do not leave senior leaders in the dark.

2. **U.S. defense leaders should establish a working definition of a quantum advantage that is not purely academic and recognizes the global strategic nature of the competition.** A "quantum advantage" for the DOD would evaluate the comparative technological positions of the United States and adversaries like China with respect to their QIST efforts. This comparative assessment offers a far more practical understanding of "quantum advantage" because it honors the global strategic nature of the competition. This definition, unlike the more academic one, also recognizes that quantum advantage is not a "zero-day" event but rather a marathon.
3. **Policymakers should not rely on subject matter experts alone to evaluate the viability of proposed QIST applications.** Senior leaders must be equipped to press engineers on everything, including qubit coherence times; qubit overhead; logical qubits; power, size, and cooling requirements; and the overall ruggedness of the quantum system. When it comes to quantum technologies, the details matter, and warfighters must be part of these assessments.
4. **Policymakers should understand and consider the benefits and drawbacks of each modality and its qubits so that they may make informed decisions regarding how to best match modalities to their use cases.** While some modalities may be more flexible and have benefits across a variety of applications, there is no single best modality. This means that senior leaders must be discerning when evaluating which modalities best match operational use cases. For example, the superconducting modality is probably not ideal for fighter aircraft applications. As with any technical design, policymakers must understand the tradeoffs between capability, cost, complexity, size, and operational utility of quantum modalities.
5. **Defense leaders must have a solid foundation in quantum science to appropriately contextualize the operational and strategic implications of Chinese technology demonstrations.** China is aggressively pursuing quantum applications, including computation, quantum key distribution, and radar. While some of this is strategic peacocking, other quantum demonstrations are indicative of a clear commitment to solving the difficult problems of fielding useful quantum applications. A knowledge of the science can help policymakers evaluate Chinese developments. For example, some claims, such as quantum radar, appear intimidating and worrisome but are most likely empty bluster. Other very public demonstrations, such as QKD, may not have apparent use cases but clearly prove that China is dedicated to working through many of the scientific and engineering challenges to fielding a broad array of quantum capabilities. Senior leaders must take Chinese developments in quantum computing seriously and consider their potential strategic consequences.

Conclusion

Understanding the basics of quantum will enable senior leaders and decision-makers to make smart choices when it comes to funding research and development, prioritizing programs, and focusing resources. This means championing and aggressively pursuing near-term applications that can deliver effects for warfighters. Candidates include timing, navigation, and certain sensing technologies. These achievable and capabilities can solve real vulnerabilities, like GPS denial, that warfighters are likely to face. Moreover, accelerating these near-term use cases for QIST will benefit the entire ecosystem of quantum capabilities because of the overlap with many of the classical, supporting hardware systems, like computer chips.

The second paper of this quantum series is a primer on quantum computing to provide senior defense leaders with an understanding of the different types of quantum computers and their properties and to establish a knowledge base from which to evaluate these machines. The third report builds on the first two, focusing on how to cultivate the quantum defense industrial base to provide U.S. warfighters a quantum advantage in a peer conflict. Procuring a quantum advantage comes down to fielding useful technologies that will provide warfighters a combat advantage, and that means cultivating an industrial base that can deliver pragmatic and effective capabilities at scale.

The nature of the strategic quantum competition with China does not give U.S. defense officials the luxury of time. DOD must accelerate the maturation of critical quantum technologies for defense—China will gladly surpass the U.S. quantum enterprise if we slow down. The DAF must take action now to help its leaders understand the underlying science needed to make choices that deliberately build up a robust and innovative quantum industrial base. **Senior leaders who can make informed decisions on high-potential, high-payoff QIST applications can provide future warfighters with a combat edge**. ✪

Endnotes

1 Paul Scharre and Ainikki Riikonen, *Defense Technology Strategy* (Washington, DC: Center for a New American Security, November 2020).

2 The Than Hoa Bridge is an excellent example of the value of precision. For over seven years and 871 sorties, general purpose, unguided bombs failed to collapse the bridge, which served as a key logistical artery for North Vietnamese forces. Then, on May 13, 1972, fourteen F-4s employed early laser-guided bombs and dropped the bridge. Laser-guided bombs enabled the wing to successfully destroy a further 196 bridges, leading to "the notion of 'one bomb, one target,' which became an accepted planning factor as more advanced precision-guided weapons emerged." The convergence of other "third offset" technologies like stealth also radically decreased the demand for other support aircraft. See David A. Deptula and Doug A. Birkey, *Resolving America's Defense Strategy-Resource Mismatch: The Case for Cost-Per-Effect Analysis* (Arlington, VA: The Mitchell Institute for Aerospace Studies, July 2020), p. 7.

3 Suzanne Folsom and Robert Garretson, "The Continuing Danger of Academic Espionage," *Inside Higher Ed*, May 4, 2020; and "China: The Risk to Academia," FBI factsheet, v2-07, 2019. Also see "The China Threat," FBI.gov.

4 "Quantum Technology Monitor," McKinsey & Company, April 2023.

5 For more, see John Stillion and Bryan Clark, *What It Takes to Win: Succeeding in 21st Century Battle Network Competitions* (Washington, DC: Center for Strategic and Budgetary Assessments, 2015).

6 Subcommittee on Quantum Information Science, Committee on Science, The National Science & Technology Council, *Bringing Quantum Sensors to Fruition* (Washington, DC: The National Science & Technology Council March 2023).

7 "What is the Impact of Quantum Computing on Cybersecurity?," Quantum Xchange blog.

8 Kelley M. Sayler, *Emerging Military Technologies: Background and Issues for Congress* (Washington, DC: Congressional Research Service (CRS), updated October 21, 2021).

9 "Celebrating Penn Engineering History: ENIAC," University of Pennsylvania.

10 "About the National Quantum Initiative," Quantum.gov.

11 H.R.6227 National Quantum Initiative Act, 115th Congress, 2017–2018.

12 H.R.6227 National Quantum Initiative Act.

13 "The Quantum Consortium: Enabling the Quantum Ecosystem."

14 "About the National Quantum Initiative"; and "Advancing American Leadership in Quantum Technology," hearing of the Committee on Science, Space, and Technology, June 7, 2023.

15 "Quantum Technology Monitor."

16 Rebel Brown, "Why Quantum Advantage & Supremacy Aren't That Complex," Quantum Computing Inc. blog. These definitions are so tightly scoped that Google declared quantum supremacy in 2019. Yet there are reasons to remain skeptical regarding the practicality of such a definition, and quantum scientists are beginning to propose alternatives to what is so clearly an academic goal. These include "quantum utility," which compares quantum computers to the equivalent units of classical hardware, or throwing out the notion of "supremacy" completely and simply recognizing that quantum computing characteristics are different than classical computers, and matching quantum computers to appropriate problem sets. Mark Mattingley-Scott and Marcus Doherty, "Why quantum 'utility' should replace quantum advantage," *TechCrunch*, November 11, 2021.

17 Defense Science Board (DSB), *Executive Summary of the DSB Report on Applications of Quantum Technologies* (Washington, DC: DOD, October 2019).

18 "The Second Quantum Revolution," National Institute of Standards and Technologies (NIST), April 5, 2022.

19 Jonathan P. Dowling and Gerard J. Milburn, "Quantum technology: the second quantum revolution," *Philosophical Transactions of the Royal Society A* 361, no. 1809, June 20, 2003; Daniel Garisto, "The Second Quantum Revolution," *Symmetry Magazine*, January 12, 2022.

20 Cory Chu, "What is Quantum Mechanics? Why it is called Quantum?—An Introduction to Quantum Mechanics," *GWLab* blog, December 9, 2021.

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

22 Daisy Dobrijevic, "The double-slit experiment: Is light a wave or a particle?," *Space.com*, March 23, 2022.

23 Garisto, "The Second Quantum Revolution."

24 Morin, "Introduction to Quantum Mechanics"; and "Collapse of the wave function," *Quantum Physics Lady: Encyclopedia of Quantum Physics*, March 10, 2019. Collapsing the wavefunction destroys the superposition of the particle into a classical state. Although uncertainty is a core principle of quantum physics, this classical state is important for quantum computation and other applications. For example, measuring, or collapsing, the wavefunction of the qubit will result in a classical bit value of 0 or 1. This collapsed state is called an eigenstate, and its value, also known as an observable, is called an eigenvalue. Olimpia Lombardi and Dennis Dieks, "Modal Interpretations of Quantum Mechanics," *Stanford Encyclopedia of Philosophy*, revised October 8, 2021.

25 This conundrum is called the "measurement problem," where physicists do not have an explanation as to why and how the waveform collapses. Different interpretations of quantum physics try to explain this mystery differently. Unified quantum physics does not have a theory as to why measurement collapses the waveform and also struggles to explain entanglement. Modal theories (there are many variations within this approach) are one line of

work that has grappled with these theoretical relationships and experimental findings. In general, modal interpretations propose that particles have "dynamical states" and "value states," where the value state is effectively a point-in-time measurement of the dynamical state and does not collapse the wavefunction. Physicists are striving to understand the seeming inconsistencies of the measurement problem, and explanations that seek to resolve it can themselves pose very strange consequences, such as parallel universes, randomness, "non-absoluteness," and the "many worlds" proposal. The measurement problem is interesting, but at this stage, it does not impact what defense leaders should know to sort through the many proposals and technologies they must manage. Anil Ananthaswamy, "Quantum Theory's 'Measurement Problem' May Be a Poison Pill for Objective Reality," *Scientific American*, May 22, 2023; and Yannis Delmas-Rigoutsos, "Quantum modalities, interpretation of Quantum Mechanics and Special Relativity, and an experimental test for multiple worlds," *HAL*, 2019.

26 Physicists do not actually know whether matter is made of particles or waves. While scientists can directly observe particles, wavefunctions most accurately describe their behavior and attributes; this is a fundamental mystery that science has yet to solve. Ananthaswamy, "Quantum Theory's 'Measurement Problem' May Be a Poison Pill for Objective Reality"; and Delmas-Rigoutsos, "Quantum modalities, interpretation of Quantum Mechanics and Special Relativity, and an experimental test for multiple worlds."

27 Dominic Walliman, "If You Don't Understand Quantum Physics, Try This!," *Domain of Science* on YouTube, February 25, 2019.

28 "A Glance at the Second Quantum Revolution," Quantum Telecommunications Italy, May 4, 2022.

29 "What Is the Uncertainty Principle and Why Is It Important?," *Caltech Science Exchange*.

30 Adam Mann, "Schrödinger's cat: The favorite, misunderstood pet of quantum mechanics," *Live Science*, February 28, 2020.

31 "The Superposition Principle," GMU.edu.

32 "If You Don't Understand Quantum Physics, Try This!"; and Indu Satija, "Being in Two Places at Once–Quantum Superposition; Macroscopic Superposition; Quantum Measurement: The Enigma of Measurement: Detecting the Quantum World; Many World Interpretation of Quantum Mechanics," class notes, GMU.edu, March 28. 2018.

33 "EdX Quantum Teleportation," *Quantum Computing* on YouTube, September 20, 2021.

34 "Eigenvalues and eigenstates in quantum mechanics," *Professor M Does Science* on YouTube, July 1, 2020.

35 Paul Penfield, Jr., "13.7: No Cloning Theorem," available via MIT OpenCourseWare.

36 William K. Wootters and Wojciech H. Zurek, "The No-Cloning Theorem," *Physics Today* 62, no. 2, February 1, 2009.

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

38 Morin, "Introduction to Quantum Mechanics."

39 Gavin Wright, "Quantum Interference," WhatIs.com, February 2023.

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

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

42 "Nonlocality and Entaglement," The Physics of the Universe; and "Modal Interpretations of Quantum Mechanics."

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

44 Ethan Siegel, "No, We Still Can't Use Quantum Entanglement To Communicate Faster Than Light," *Forbes*, January 2, 2020.

45 "Nonlocality and Entaglement."

46 Ahmed Banafa, "Quantum Teleportation: Facts and Myths," *OpenMind*, February 1, 2021.

47 "EdX Quantum Teleportation."

48 "EdX Quantum Teleportation."

49 DSB, Executive Summary of the DSB Report on Applications of Quantum Technologies.

50 Elise Crull, "Quantum Decoherence," draft, *Routledge Companion to Philosophy of Physics*, April 14, 2018.

51 "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.

52 Katherine McCormick, "Decoherence Is a Problem for Quantum Computing, But ..." *Scientific American*, March 30, 2020.

53 Robert Konik, "Quantum coherence confined," *Nature Physics*, March 18, 2021.

54 "1953: Transistorized Computers Emerge," The 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. The next generation of computer hardware would use integrated circuits and microprocessors. Advances in material science and physics have enabled the rapid and dramatic improvement of microprocessors that many people understand as "Moore's law": the number of transistors on an integrated circuit doubles 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 17nm due to cost/value tradeoffs). At approximately 7nm, 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 Magazine*, May 20, 2022; and Heidi Vella, "Quantum for dummies: the basics explained,"

Engineering and Technology Magazine, April 16, 2019.

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

56 "EdX Quantum Teleportation."

57 "Quantum Programming - Part 1."

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

59 "The Map of Quantum Computing - Quantum Computing Explained."

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

61 "The Map of Quantum Computing - Quantum Computing Explained."

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

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

64 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.

65 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 assign 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 Lombardi and Dieks, "Modal Interpretations of Quantum Mechanics."

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

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

68 "Gates" are basic circuit operations that control how computers physically process the bits of information to calculate algorithms. For classical computers, this is literally opening or closing the electrical circuit, where a 1 allows the electrical current to flow, and a 0 blocks the current. The physical sequence and design of the circuit board enable simple or complex algorithms. The problem with classical gates is that they lose information when processing the qubits. That is, because of superposition, one cannot know whether the first or second qubit is in the 1 or 0 state. Moreover, they are irreversible. Once the information is processed through the gate, it cannot be recovered. Classical gates include logical functions such as "and," "or," "not," and so forth.

69 Quantum logic gates control unique quantum properties like spin, phase, and superposition. Simplistically, one can visualize quantum gates as manipulating the vector of the Bloch Sphere. Although many quantum logic gates can function like classical gates, quantum gates are reversible and do not lose information in the system. Perhaps most importantly, quantum gates can perform their functions without collapsing the wavefunction. Completing these computations without collapsing or only selectively collapsing the superposition of qubits is a major factor in the power of quantum computers. Some quantum gates are analogs of classical logic gates, but others exploit the unique quantum properties of qubits.

70 "Quantum Computing Hardware - An Introduction."

71 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. Korey Haynes, "How cold is it in outer space?," *Astronomy*, February 28, 2020.

72 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.

73 J.S. Tsai, Y. Nakamura, and Yu. Pashkin, "Superconducting single-Cooper-pair box as quantum bit," *Physica C: Superconductivity*, September 2001; "Superconducting Qubit," *NTT SCL* on YouTube, August 16, 2015; and John Clarke and Frank K. Wilhelm, "Superconducting quantum bits," *Nature*, June 18, 2008.

74 Mooij, "Superconducting quantum bits." Charge qubits require Cooper pair boxes to manipulate and measure the qubit. Flux and phase qubits use the direction of charge flow in the circuit. Clockwise is a value of 0, and counterclockwise is 1. Because the circuit is superconducting, charge can flow both ways, representing a superposition. "What is a qubit?" Universtiy of Waterloo. There are more specialized types of qubits that belong to these three categories but are not necessary to cover in this overview.

75 Other factors, such as the chip manufacturing quality or the precision of control systems, may also impact their choice of chip design (and, by extension, qubit type).

76 "Quantum Computing Hardware and Platforms | Superconducting Qubits, Trapped Ions, Majorana," *Anastasia Marchenkova* on YouTube, June 29, 2021.

77 "Quantum Computing Hardware - An Introduction."

78 Philip Krantz et al., "A Quantum Engineer's Guide

to Superconducting Qubits," *Applied Physics Reviews*, July 7, 2021.

79 Rosalie Chan, "IBM unveils the world's first quantum computer that businesses can actually use to solve previously impossible problems," *Business Insider*, January 13, 2019.

80 Russ Fein, "Quantum Computing Modalities – A Qubit Primer Revisited," *The Quantum Leap* blog, October 20, 2022.

81 Michael James Martin et al., "Energy use in quantum data centers: Scaling the impact of computer architecture, qubit performance, size, and thermal parameters," National Renewable Energy Laboratory, March 30, 2021.

82 Chris Woodford, "What are quantum dots?" Explainthatstuff.com, 2012/2023.

83 M.A. Eriksson , S.N. Coppersmith , and M.G. Lagally, "Semiconductor quantum dot qubits," *MRS Bulletin*, October 2013.

84 Mark Leal, "Quantum Dots and their Application as Electron Spin Qubits," Aim Academy Photonics, May 29, 2021.

85 For a far more detailed and accessible description of neutral atom modality, computation, strengths, and challenges, see Karen Wintersperger et al., "Neutral Atom Quantum Computing Hardware: Performance and End-User Perspective," *EPJ Quantum Technology*, August 28, 2023.

86 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.

87 "Pasqal neutral atoms," *Pasqal Quantum Computing* on YouTube. January 2, 2022.

88 Edd Gent, "IBM's 127-Qubit Eagle Is the Biggest Quantum Computer Yet," *Singularity Hub*, November 22, 2021.

89 "Building Scalable Quantum Computers from Arrays of Neutral Atoms."

90 Somoroff et al., "Millisecond coherence in a superconducting qubit," Department of Physics, Joint Quantum Institute, and Center for Nanophysics and Advanced Materials, University of Maryland, March 15, 2021.

91 Gent, "IBM's 127-Qubit Eagle Is the Biggest Quantum Computer Yet"; John Russell, "Quantum Watch: Neutral Atoms Draw Growing Attention as Promising Qubit Technology," *HPC Wire*, January 25, 2022.

92 Loïc Henriet et al., "Quantum Computing with Neutral Atoms," *Quantum* 4, no. 327, September 18, 2020.

93 Wintersperger et al., "Neutral Atom Quantum Computing Hardware."

94 DSB, Executive Summary of the DSB Report on Applications of Quantum Technologies.

95 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.

96 Jungsang Kim, "Trapped Ions Make Impeccable Qubits," *Physics* 7, no. 119, November 24, 2014.

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

98 C. Monroe and Jungsang Kim, "Scaling the Ion Trap Quantum Processor," *Science*, March 2013. Hybrid approaches that employ trapped ions on a photonic chip may enable scalability that uses the best of both modalities. This research is still nascent and, importantly, focused on computation. Robert J. Niffenegger et al., "Integrated multi-wavelength control of an ion qubit," *Nature*, January 3, 2021.

99 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.

100 Peter Lodahl, Arne Ludwig, and Richard J. Warburton, "A deterministic source of single photons," *Physics Today* 75, no. 3, March 2022.

101 Galan Moody et al., "Roadmap on Integrated Quantum Photonics," *Journal of Physics: Photonics*, 2021; and Sergei Slussarenko and Geoff J. Pryde, "Photonic quantum information processing: A concise review," *Applied Physics Reviews* 6, no. 4, December 2019.

102 Lodahl, Ludwig, and Warburton, "A deterministic source of single photons."

103 Rob Matheson, "Generating high-quality single photons for quantum computing," *MIT News*, May 14, 2019.

104 Wim Bogaerts et al., "Programmable photonic circuits," *Nature*, October 7, 2020.

105 University of Southern California, "Quantum Photonics Breakthrough Promises a New Era of Powerful Optical Circuits," *SciTechDaily*, April 10, 2021.

106 Wintersperger et al., "Neutral Atom Quantum Computing Hardware."

107 Universität Paderborn, "Integrated photonics for quantum technologies," *Phys.org*, January 7, 2022; Jeremy O'Brien, Akira Furusawa, and Jelena Vuckovic, "Photonic quantum technologies," *Nature Photonics*, March 2010; and Moody et al., "2022 Roadmap on integrated quantum photonics."

108 "Betting big on quantum," McKinsey & Company, September 13, 2022.

109 Mateusz Masiowski, Niko Mohr , Henning Soller , and Matija Zesko, "Quantum computing funding remains strong, but talent gap raises concern," McKinsey & Company, June 15, 2022. Quantum radar is just one example of how China is looking to use QIST for military use. See Stephen Chen, "Chinese team says quantum physics project moves radar closer to detecting stealth aircraft," *South China Morning Post*, September 3, 2021.; and Joseph Trevithick, "China Reveals Prototype Configuration of Jam Resistant and Counter-Stealth 'Quantum Radar'," *The Warzone* blog, November 6, 2018.

110 “Micius Quantum Communication Satellite,” Aerospace Technology.

111 Karen Kwon, “China reaches new milestone in space based quantum communications,” *Scientific American*, June 25, 2020.

112 Juan Yin et al., “Entanglement-based secure quantum cryptography over 1,120 kilometres,” *Nature*, June 15, 2020.

113 “Quantum Key Distribution (QKD) and Quantum Cryptography (QC),” National Security Agency/Central Security Service; and Koji Azuma et al., “Quantum repeaters: From quantum networks to the quantum internet,” July 19, 2023.

114 University of Science and Technology of China, “The world’s first integrated quantum communication network,” *Phys.org*, January 6, 2021.

115 Lee Billings, “China Shatters ‘Spooky Action at a Distance’ Record, Preps for Quantum Internet,” *Scientific American*, June 15, 2017.

116 Charles Q. Choi, “Two of World’s Biggest Quantum Computers Made in China,” *IEEE Spectrum*, November 6, 2021.

117 François Candelon, Maxime Courtaux, Gabriel Nahas, and Jean-François Bobier, “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.

118 Emily Conover, “Google claimed quantum supremacy in 2019—and sparked controversy,” *Science News*, December 16, 2019.

119 Jamilah Lim, “China’s quantum computing efforts surpasses the West’s – again.” *Techwire Asia*, November 3, 2021; 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); and Choi, “Two of World’s Biggest Quantum Computers Made in China.”

120 Patrick Tucker, “Is China About to Destroy Encryption As We Know It? Maybe,” *Defense One*, January 20, 2023; Bao Yan et al., “Factoring Integers with Sublinear Resources on a Superconducting Quantum Processor,” December 23, 2022.

121 Tucker, “Is China About to Destroy Encryption As We Know It? Maybe.”

122 “China Shows Off First Quantum Radar Prototype,” *Aviation Week*, November 5, 2018.

123 Chen, “Chinese team says quantum physics project moves radar closer to detecting stealth aircraft.”

124 Brad Bergan, “China Is Reportedly Developing Quantum Radar to Detect Stealth Jets,” *Interesting Engineering*, September 3, 2021; “China Shows Off First Quantum Radar Prototype”; and Adrian Cho, “The short weird life—and potential afterlife—of quantum radar,” *Science*, September 23, 2020.

125 Cho, “The short weird life—and potential afterlife—of quantum radar.”

126 The theory behind quantum radar is that one of a pair of entangled photons is emitted, while the other is held in storage. When the entangled photon hits a stealth aircraft, it changes that photon, which then also changes the stored partner. Thus, even if a photon is deflected to a different direction and does not return to the originating radar, an object could be detected well below environmental “noise.” Major pragmatic challenges to this concept are that quantum storage is still early in development and one cannot “monitor” the stored photon without collapsing it and the entanglement. It is also unclear how a quantum radar would be able to translate these into target ranges or a target track.

127 OSD, Military and Security Developments Involving the People’s Republic of China 2021, annual report to Congress (Washington, DC: DOD, November 3, 2021).

128 James Jin Kang, “The Thousand Talents Plan is part of China’s long quest to become the global scientific leader,” *The Conversation*, August 31, 202; and U.S. Senate, Permanent Subcommittee on Investigations, Committee On Homeland Security And Governmental Affairs, *Threats to the U.S. Research Enterprise: China’s Talent Recruitment Plans*, staff report (Washington, DC: U.S. Senate, November 18, 2019).

129 Alex Joske, *Hunting the Phoenix* (Canberra: Australian Strategic Policy Institutue, August 20, 2020). In 2018, recognizing the sensitivity of the United States to these efforts, the CCP put out official guidance to avoid the use of emails for communication and not mention the “Thousand Talents Plan” in their activities.

130 See Joske, Hunting the Phoenix. This report provides case studies of Chinese recruitment activities.

131 Ralph Jennings, “Why China’s Advancements in Quantum Technology Worry Others,” *Voice of America*, December 14, 2021; and “China’s 14th Five-Year Plan,” Issue Brief, United Nations Development Programme, July 23, 2021.

132 “Quantum Technology Monitor.”

133 China Power Team, “Is China a Leader in Quantum Technologies?” *China Power*, updated August 16, 2023.

134 Jakob Pii, “Chinese Quantum Companies And National Strategy 2023,” *The Quantum Insider*, April 13, 2023.

135 John Prisco, “China: The Quantum Competition We Can’t Ignore,” *Forbes*, January 21, 2021.

136 Daniel Garisto, “China is Pulling Ahead in Global Quantum Race, New Studies Suggest,” *Scientific American*, July 15, 2021.

137 “Quantum Technology Monitor.”

138 “Quantum Technology Monitor.”

139 Jeff Pao, “China’s fastest yet quantum computer still way behind US,” *Asia Times*, June 9, 2023.

140 Abraham Mahshie, “Kendall: ‘Race For Technological Superiority With China’ Warrants Divestments,” *Air & Space Forces Magazine*, May 17, 2022.

141 Mahshie, “Kendall: ‘Race For Technological Superiority With China’ Warrants Divestments.”

142 “Chinese Threats in the Quantum Era,” Booz Allen Hamilton; Brandi Vincent, “Report: China May Steal Encrypted Government Data Now to Decrypt with Quantum Computers Later,” *NextGov FCW*, November 22, 2021.

Glossary

adiabatic quantum computing: This kind of computing presents a way of organizing a quantum computer that is different from a circuit model based on quantum gates. This computation uses an algorithm that tracks the gradual transformation of a system, or Hamiltonian, with a known ground state at a controlled rate and is used to solve optimization problems.

atomic energy levels: In classical physics and chemistry, atomic energy levels correspond to the orbit of a particular electron. Electrons can absorb the energy of photons and jump to a higher energy level. They can also emit photons and fall to a lower energy level. The lowest energy level is referred to as the ground state, and higher energy levels are referred to as excited states.

Bose-Einstein condensate (BEC): At extremely low temperatures approaching absolute zero, bosons will collapse to the lowest energy level, or ground state, to form a state of matter referred to as a Bose-Einstein condensate. This state is useful because all atoms in the condensate exhibit the same quantum effects, allowing experiments to be conducted at a larger scale.

boson: A boson is a type of subatomic particle, and gauge bosons, such as photons, are fundamental particles, meaning they are not made up of smaller particles. Bosons have whole integer spins such as 0, 1, -1, 2, and -2, a property that allows them to occupy the same quantum state, meaning they do not adhere to the Pauli exclusion principle like their fermion counterparts. At extremely low temperatures, bosons can collapse to the lowest energy level, or ground state, to form a Bose-Einstein condensate.

Cooper pair: A Cooper pair is a "quasi-particle," or composite boson, made of coupled electrons with opposite momenta. While individual electrons are fermions with ½ spins and follow the Pauli exclusion principle, Cooper pairs behave like bosons and have a total spin that is a whole integer like 0 or 1, so they can similarly be condensed into a quantum collective wave, a condensate that forms the basis of superconductivity.

Copenhagen interpretation: The Copenhagen interpretation is a standard theoretical framework of quantum mechanics that states a quantum system is in superposition in accordance with the probability distribution of its wave function. In other words, a quantum particle doesn't exist in one state or another but all states until the moment of observation.

decoherence: Decoherence is a basic quantum principle describing the loss of a qubit's quantum properties, such as its entanglement or superposition—its coherence—over time due to quantum noise. In an uncontrolled environment, this occurs near-instantaneously. Carefully controlled environments in a quantum device extend the coherence of a quantum particle but are still vulnerable to interference from measurement devices, containers, the external environment, and other quantum particles. Some particles are more or less vulnerable to interference.

eigenstate: The eigenstate describes the characteristics of a quantum particle in terms of vectors. For instance, an electron can have one of two eigenstates after measurement, including "spin up" and "spin down."

eigenvalue: An eigenvalue is the value of an eigenstate, also known as an observable. In the basic equation $Ax = \lambda x$, the number or scalar value "λ" is an eigenvalue of the eigenstate "A."

entanglement: Entanglement is a relationship between two or more particles such that one cannot be described or measured without impacting the quantum state of all entangled particles, even when separated by large distances or having no other physical connection. This property allows an observer to predict the quantum state of other systems. Entanglement can occur both in nature and intentionally. There are four ways in which particles can become entangled: through initial creation or emission of photons; through "second-generation" entanglement, using entangled photons to entangle other particles; by "accident," or based on probability; and through intentional nearby interaction, for example by exciting particles with a laser.

fermion: Fermions are a type of subatomic particle and include electrons, protons, and quarks. These particles have ½ spins and have values such as 1/2, -1/2, 3/2, and -3/2. As a result, they adhere to the Pauli exclusion principle, meaning that no two particles can occupy the same quantum state. However, pairing fermions can create a composite boson since, mathematically, adding two halves together makes a whole integer.

gate-based quantum computing: Gate-based quantum computing performs operations by using logic gates analogous to those of a classical computer. These gates manipulate the state of qubits in order to perform computations. Compared to the quantum annealing method, gate-based quantum computing can be used in a wider variety of applications beyond optimization problems.

ground state: Atoms are in the ground state when their electrons occupy the lowest possible combination of energy levels. When electrons are temporarily elevated from the ground state to a higher energy level, atoms are considered to be in an excited state.

Grover's algorithm: Grover's algorithm is a type of quantum search and optimization algorithm that can be applied to large, unstructured datasets. This offers the potential for significant speedups that may one day enable the rapid breaking of existing encryption protocols. However, performing this function requires memory beyond what is available in existing devices.

Hamiltonian: A Hamiltonian is a mathematical description of a system in terms of energy states—in other words, both its kinetic and potential energy—and represents the total energy of a system. A "system" can be a qubit, an atom, or even an object like the moon.

Hilbert space: A Hilbert space is a mathematical construct: a vector space that contains all possible functions that can describe a quantum system.

identical and indistinguishable particles: Identical particles are those that always have the same properties. For instance, every electron will always have a negative charge. Classical identical particles can still be individually identified because their position and velocity are continually observable. On the other hand, quantum particles are both identical and indistinguishable because their position and velocity are described by a probability distribution and are not continually observable.

Josephson junction: A Josephson junction is a device composed of a gap or insulator separating two superconducting regions. They are foundational to the operation of a superconducting quantum computer, where the behavior of cooper pairs tunneling through the barrier is the subject of measurement.

microcomb: Microcombs are experimental devices that are used to produce entangled light waves for quantum technology applications.

modality: A modality is a particular technique or pathway used to prepare and preserve qubits for quantum operations. Each has its own advantages and drawbacks. Some of the most commonly employed modalities are superconducting, trapped ion, neutral or cold atom, and silicon or quantum dot.

neutral atom qubits: Neutral atom qubits use lasers to trap and cool atoms to extremely cold temperatures while organizing them into a two or three-dimensional grid. This approach offers large advantages in coherence time and resistance to noise and does not have the hardware or power footprint of other cooling-based modalities. These features make this modality a good candidate for mobile applications if the underlying hardware can be miniaturized.

Pauli exclusion principle: This principle states that no two fermions, such as electrons, can occupy the same orbital and quantum state. This means that every energy level in an atom can only have either one electron or two electrons of opposite spins. Bosons and composite bosons made of coupled fermions do not adhere to this principle.

photonic integrated circuit: Photonic integrated circuits are devices that use photons as the fundamental basis of information transfer across a circuit. They differ from traditional microelectronics that use electrons in the same manner. These photons are introduced to the system from a laser, manipulated through circuit designs like switches and interferometers, and measured. Like traditional electronics, these can be operated at room temperature.

photonic qubits: Photonic qubits are the basis of the photon-based computing modality as well as quantum communications. Photonic quantum computers operate by generating photons using a laser, standardizing them in a particular state, manipulating their polarization, and conducting measurements. Using photonic qubits as a modality has several advantages, including the ability to operate at room temperature, traverse space as "flying qubits" without decohering, and exploit existing manufacturing technologies. However, photonic qubits are difficult to entangle and modify, and they are limited by the effectiveness of measurement devices.

polarization: Polarization is a property of photons defined by the shape and orientation of light waves in relation to the direction of travel. Just as electrons can be interpreted by their spin, photons can be measured by their polarization. In devices such as a photonic integrated circuit, polarization can be altered in order to perform operations on photonic qubits.

quantum accelerometer: A quantum accelerometer is a device that measures linear acceleration by detecting shifts in the quantum states of atoms that are induced by motion. This enables precise inertial navigation by eliminating the errors inherent in existing mechanical accelerometers.

quantum advantage: A quantum advantage describes a situation in which a quantum device outperforms classical counterparts in a specific function or application. For example, in quantum computing, this means solving a problem that would take an impractical length of time for the most advanced, specialized classical computers.

quantum artificial intelligence (AI) and machine learning (ML): This is the application of quantum computing to improve the efficiency of AI and machine learning mathematical processes. It takes advantage of quantum computing's speed in completing mathematic tasks like optimization, sampling, and linear algebra. Similarly, the application of quantum neural networks can improve pattern recognition with sparser data.

quantum algorithm: Quantum algorithms outline the rules and processes to complete an operation using a quantum computer. They provide increased speeds over classical algorithms by leveraging quantum effects. Examples include Shor's algorithm for factorization and Grover's algorithm for search and optimization.

quantum annealing: Quantum annealing is a computational method involving gradual evolution toward a final state. It is useful for optimization problems like traffic planning or finance. Compared to the gate-based method of quantum computing, quantum annealing is far more scalable but less flexible.

quantum circuit: A quantum circuit is a sequence of interconnected quantum gates that performs operations on qubits for the purpose of computation. They are analogous to classical logic circuits but can perform additional gate operations and are reversible.

quantum clock: A quantum clock indexes quantum properties like miniscule transitions between atomic energy levels. They are distinct from existing atomic clocks, which often rely on measuring the radioactive decay of cesium because they measure quantum changes within atoms with orders of magnitude greater precision. Networks of quantum clocks may also be used as a backup for satellite-based GPS clocks or as a means of detecting subtle changes in Earth's gravitational field.

quantum communications: At current technology levels, quantum communication is centered around Quantum Key Distribution. This is a process by which a cryptographic key is transmitted between two parties to encrypt information. If a third party attempted to obtain the key by manipulating the qubits, it would collapse its entanglement and alert the sender and receiver. However, with current capabilities, classical information must be transmitted classically, and achieving range would require the extension of trusted repeaters.

quantum computing: Quantum computing is the application of quantum phenomena such as superposition and entanglement to perform computation. Qubits form the fundamental unit of information. Quantum computing has the potential to either perform classical functions extremely efficiently or enable entirely new capabilities like simulating quantum systems.

quantum cryptography: Quantum cryptography is the application of quantum mechanical properties to perform cryptographic tasks like Quantum Key Distribution, encryption, and decryption.

quantum error correction: Quantum Error Correction consists of techniques to protect quantum information from noise and decoherence. One avenue of quantum error correction uses additional redundant qubits to encode logical qubits with standardized states.

quantum gate: Quantum gates perform computational operations using qubits. Common gates include X, Y, Z, Hadamard, Phase Shift, CNOT, and SWAP. Many are analogous to classical logic gates like AND, OR, and NOT and are reversible.

quantum gravimeter: A quantum gravimeter is a device that uses techniques like matter-wave interferometry to obtain precise measurements of gravitational acceleration. This method can be used to create precise maps of surface, underground, and undersea features.

quantum gyroscope: A quantum gyroscope is a sensor that precisely measures rotation and acceleration with great accuracy by analyzing interference contributing to a quantum state. In one example, using atom interferometry, two clouds of atoms in an excited or ground state traverse a series of lasers. One cloud will travel further through the test area due to the effects of external rotation and acceleration. Measuring this difference allows for precise information on the device's movement. In combination with other sensors, this device can provide the basis for a quantum inertial navigation system.

quantum imaging: Quantum imaging is a process that takes advantage of the properties of photons to achieve higher resolution or indirect images. One example includes ghost imaging, which interprets a photon that has interacted with an object by measuring a displaced but spatially correlated photon.

quantum magnetometer: A quantum magnetometer is an ultra-sensitive device used to measure magnetic field strength, allowing for the creation of precise maps for navigation or sensing or the discovery of resource deposits. One promising application is for undersea submarine navigation in the absence of GPS.

quantum memory: Quantum memory is a theoretical device that would provide the capability to store and reproduce a previously established quantum state in a qubit. This is essential for universal quantum computing but also to increase communication ranges and perform operations or computations that require referencing previous qubit information.

quantum network: A quantum network is a system that allows the transmission of quantum information between two or more nodes. Linkages can be physical, such as fiberoptic lines, or wireless through methods such as satellite transmission. A network is required for applications like Quantum Key Distribution (QKD).

quantum neural network: Neural networks are a method of machine learning that imitates the ways we currently understand the human brain to process information. Inputs are processed through a series of interconnected "hidden layers" leading to an output and can be trained on data. Quantum computing benefits this process by virtue of its greater efficiency in conducting pattern searches.

quantum noise: Quantum noise is unwanted interference between a quantum system and the external environment or measurement device that leads to decoherence. This is a major barrier to the operation of some devices outside of laboratory settings or for extended periods.

quantum positioning, navigation, and timing (PNT): Quantum PNT is a sub-discipline of quantum sensing that leverages one or more sensing modalities to generate precise positioning, navigation, and timing information. This would act as a backup if satellite-based PNT was denied, and ideally, it can operate without any external data inputs. However, many of the requisite devices are not miniaturized enough to be completely portable and are also vulnerable to the noise and interference generated by a vehicle in motion.

quantum repeater: A quantum repeater enables the transmission of a quantum state over a long distance by mitigating the effects of decay and decoherence. It is analogous to a radio repeater that mitigates the effects of electromagnetic attenuation. Repeaters present the greatest vulnerability for malicious actors to interfere with a quantum network.

quantum radio frequency (RF): Quantum RF leverages the property of Rydberg atoms to be extremely susceptible to external influence to act as a receiver for radio frequency transmissions. Demonstrations have shown that quantum RF receivers can sample a very wide range of the spectrum beyond the ability of existing systems.

quantum sensing: Quantum sensing is the application of quantum properties to obtain extremely precise measurements of magnetic fields, gravity, acceleration, or other variables. Quantum sensors can be used to generate comprehensive maps of surface, underground, and undersea features for commercial, scientific, and military purposes. The combination of multiple sensing modalities can allow for assured navigation without external inputs.

quantum simulator: A quantum simulator is a single-purpose, non-programmable device designed to simulate other quantum systems for applications such as chemistry or pharmaceutical research.

quantum supremacy: Quantum supremacy is the demonstration of a quantum application that is impossible to achieve through existing methods. In quantum computing, this means the completion of a task that is impossible for a classical computer at any length of time: no classical computer can accurately and completely simulate a quantum system.

quantum system: A quantum system is any system that can be described by its quantum mechanical properties. This means that its components have no discrete values until measured, can be expressed as a wave function, and can be entangled with other components of the same type, such as electrons to electrons or photons to photons.

quantum teleportation: Quantum teleportation is the transfer of information describing a qubit's quantum state from one location to another without physically moving it. This is enabled by the property of quantum entanglement.

quantum tunneling: Quantum tunneling is the ability of a quantum system or particle to traverse a solid barrier in less time than if it traveled freely. The thickness of the barrier does not significantly impact this speed. Therefore, a sufficiently thick barrier will allow the tunneling speed to exceed the speed of light.

qubit: Qubit is the abbreviation of quantum bit. It is a binary unit of quantum information comparable to binary bits in classical computing. A qubit can represent the basis states of $|0>$, $|1>$, or a superposition of both states.

quantum key distribution (QKD): QKD is the application of quantum communications to distribute a secret encrypted key to two or more parties. Interception of the transmission would collapse the quantum state, making the key unusable and the intrusion detectable.

qubit coherence time: Qubit coherence time is the duration a qubit can maintain its quantum state before decoherence occurs. This is a key metric for quantum hardware, as longer coherence times enable more persistent operations to be performed.

Rydberg atom: Rydberg atoms are in a highly excited state and have a single electron in a high energy level. This makes them uniquely responsive to external manipulation. They are useful as a base for establishing a Bose-Einstein condensate.

Schrödinger equation: The Schrödinger equation is the foundational equation of quantum mechanics. It is used to calculate the wave function of any quantum system. The time-dependent variant of the equation is used to predict a wave function's evolution over time.

Shor's algorithm: Shor's algorithm is a quantum algorithm that calculates the prime factorization of very large numbers. Prime factorization becomes exponentially more intensive for classical computers to compute due to the lack of patterns and the need to consider solutions sequentially. Quantum computers utilizing Shor's algorithm can compute factors in parallel, offering massive speedups. This poses a threat to existing encryption protocols such as RSA.

silicon or quantum dot qubits: A quantum dot is a microscopic structure composed of semiconducting atoms such as silicon that behaves almost like a single artificial atom. The qubit in this modality is a single electron that is confined and manipulated within the dot structure. While the microelectronics industry is experienced in working with silicon-based chips, it is difficult to scale this modality due to the risk of noise interference with other nearby dots.

spin: Spin is the angular momentum of a particle, analogous but not equivalent to the classical momentum of a physical object. Electrons, for example, can be measured as "spin up" or "spin down," but prior to measurement exists in a superposition of both states.

state vector: A state vector mathematically represents the complete possible states of a quantum system, including the basis states of 0 and 1 and infinite superpositions in between. Measurement causes this superposition to collapse into one of the two basis states.

superposition: Superposition is the phenomenon where a qubit can be in multiple quantum states simultaneously. This is one of the foundational ideas that separates quantum and classical interpretations of the universe.

superconducting qubits: Superconducting qubits are a quantum modality that leverages the ability of some atoms to act as superconductors at extremely cold temperatures, meaning that electrons will face no electrical resistance when traversing a circuit. The "qubit" in this modality is the circuit itself. Electrons are entangled as Cooper Pairs that must "jump" a Josephson junction to complete the circuit. Their quantum state is modified by devices such as microwave resonators. This modality is very useful for quantum computing applications and is similar to existing computer chips in concept and manufacturing. However, it is also limited by the necessity to cryogenically cool the circuit.

trapped-ion qubits: Trapped-ion qubits are a quantum computing modality in which atoms are heated to a gaseous state, have excess electrons removed, and are fixed and supercooled by a laser. This is conceptually and operationally similar to the neutral atom modality and, accordingly, has advantages in qubit coherence time and fidelity. However, charged ions may be comparatively more vulnerable to noise or other interactions.

universal quantum computer: A universal quantum computer combines all functions of classical computers with the ability to perform the full range of logic gate functions on its operating qubits. This contrasts with existing systems, which are often tailored to a particular algorithm, function, or application, with little utility outside of this focus. In some cases, current quantum computers are not reprogrammable, as their logic gates or other devices are fixed in place to perform a specific experiment.

wave function: The wave function contains the total available information of a quantum system and is found by solving the Schrödinger Equation. It is mathematically represented by the letter Ψ (Psi). The square of the wave function represents the probability of measuring a particle as being in a particular state. This measurement collapses the wave function, making what was previously a probability distribution into a discrete state.

wave-particle duality: Wave-particle duality is a theory that states that particles can behave like waves and, conversely, that waves can behave like particles. In quantum mechanics, electrons exemplify this theory by existing in a probability distribution that acts as a wave before a measurement collapses this wave function into a particular particle with discrete properties.

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