BETTER TECH FOR TOMORROW

THE QUANTUM FRONTIER

Leading the Next Generation of Computing

WRITTEN BY
Shon Pan
May 2026

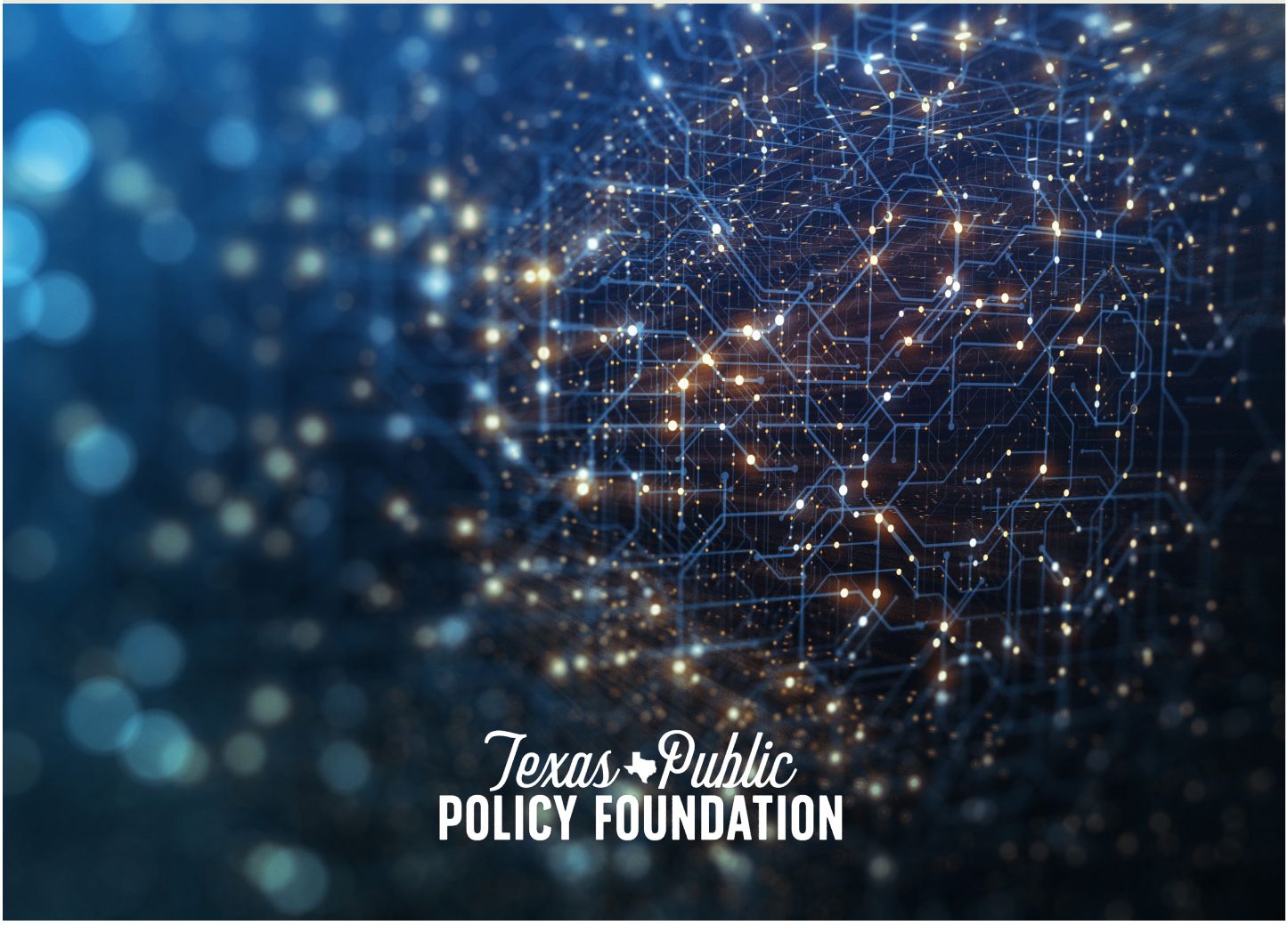


TABLE OF CONTENTS

THE QUANTUM FRONTIER

Leading the Next Generation of Computing

WRITTEN BY **Shon Pan**

KEY POINTS

- **Quantum technology** spans three verticals: computing (simulation of matter), sensing (precision measurement), and networking (secure communication).
- **The clearest near-term threat:** quantum computers will break the encryption protecting all digital infrastructure. Adversaries are harvesting data now.
- **Texas passed HB 4751**, creating a Quantum Initiative, but implementation is pending. The framework exists, but Texas must act and invest now to capture the opportunities and meet threats that quantum will deliver.
- **A workforce-first approach** using existing mechanisms (GURI, TUF) can be a carefully guided state investment that can unlock a far larger federal and private capital. Colorado demonstrated this with a 45-to-1 return.
- **Right now, quantum remains** a nascent technology, ripe for research and novel ideas to disrupt present entrants. Texas should invest in talent that transfers across approaches.

EXECUTIVE SUMMARY

The next consequential technology conversation is already here, and this time, it is not about artificial intelligence.

Quantum technology is a fundamentally different approach to conventional computing that harnesses the behavior of subatomic particles to solve problems that have been, until now, completely impossible for current computers. The implications run in two directions: enormous potential for materials technology and simulation, and major dangers to privacy that could render encryption used for anything from financial to military purposes useless. Many corporations are investing billions, and rival nations like China have committed more than $15 billion in public quantum research.

Texas, the nation's largest energy-producing state and a major hub of technological innovation, thus faces both an opportunity and an obligation. Quantum computing's advantages in simulating the behavior of matter at the atomic level can build incredible materials technology, from better solar cells to simulations of the very building materials of the universe. Quantum sensing, already commercially deployed, offers immediate value, sharpening exploration precision and protecting infrastructure in an industry that accounted for $366 billion in direct economic activity in 2024.

At the same time, Texas must prepare its critical infrastructure for a world where current encryption is no longer sufficient. Adversaries are already conducting "harvest now, decrypt later" operations, collecting encrypted data for future decryption and yet the Texas Department of Information Resources has not yet published any post-quantum guidance.

Texas is better positioned than many observers recognize. Scott Aaronson, one of the world's top quantum scientists, assesses the Texas quantum ecosystem as stronger than Colorado's

program, which itself is one of the most successful in the nation. House Bill 4751, the Texas Quantum Initiative Act, signed into law in June 2025, established a formal state framework for quantum investment.

This paper recommends a workforce-first, fiscally conservative approach to deploy existing mechanisms, including the Governor's University Research Initiative and the Texas University Fund, to build quantum talent and sustain the Texas Miracle.

I. WHAT IS QUANTUM TECHNOLOGY?

Quantum technology is the application of quantum mechanics, or physics directing subatomic particles. This particularly pays close attention to subatomic particles' exotic properties, such as *tunneling*, which allows them to (on occasion) pass through apparently solid objects; *entanglement*, where two particles are connected irrespective of distance; and *superposition*, where the particles can exist in multiple states simultaneously. Despite the counterintuitive nature of these findings, these properties have been experimentally verified by over a hundred years of experimental investigation.

This paper focuses upon the practical utility of their application: **quantum computing** (where this is used to perform calculations, such as simulating the possible or expected states of matter); **quantum networking** (where this is used for communication, such as eavesdropping-proof transmissions); and **quantum sensing** (where this is used to determine the location of items or phenomena, without needing GPS or to find reservoirs of petrochemicals).

Readers primarily interested in policy recommendations may proceed directly to Section V.

A Brief History

The Physics Foundation (1920s–1980s)

Quantum computing traces its origins to the physics revolution of the early twentieth century. It was a deceptively simple experiment: when scientists fired individual light particles known as photons at a barrier with two narrow slits, they expected them to be blocked by the barrier with some particles going through one or the other slit, akin to tiny billiard balls against a wall with small gaps. Instead, the particles appeared to go through both slits simultaneously, as if a ball was thrown against a wall and somehow exited from both gaps. They were acting as if they were a wave rather than as if they were solid objects — at least until they were measured, whereupon they reverted to expected behavior, exiting through one slit or the other. It was as if the very act of viewing something would change reality.

This revealed something profound: subatomic particles do not operate the way that familiar physical objects do. Whereas we might visualize our moon orbiting Earth in a way similar to a billiard ball circling a basketball and have the physics be roughly correct, this is not true of the way that subatomic electrons orbiting an atom behave. They act more like a cloud of possibilities, existing in many states at once, until they are measured.

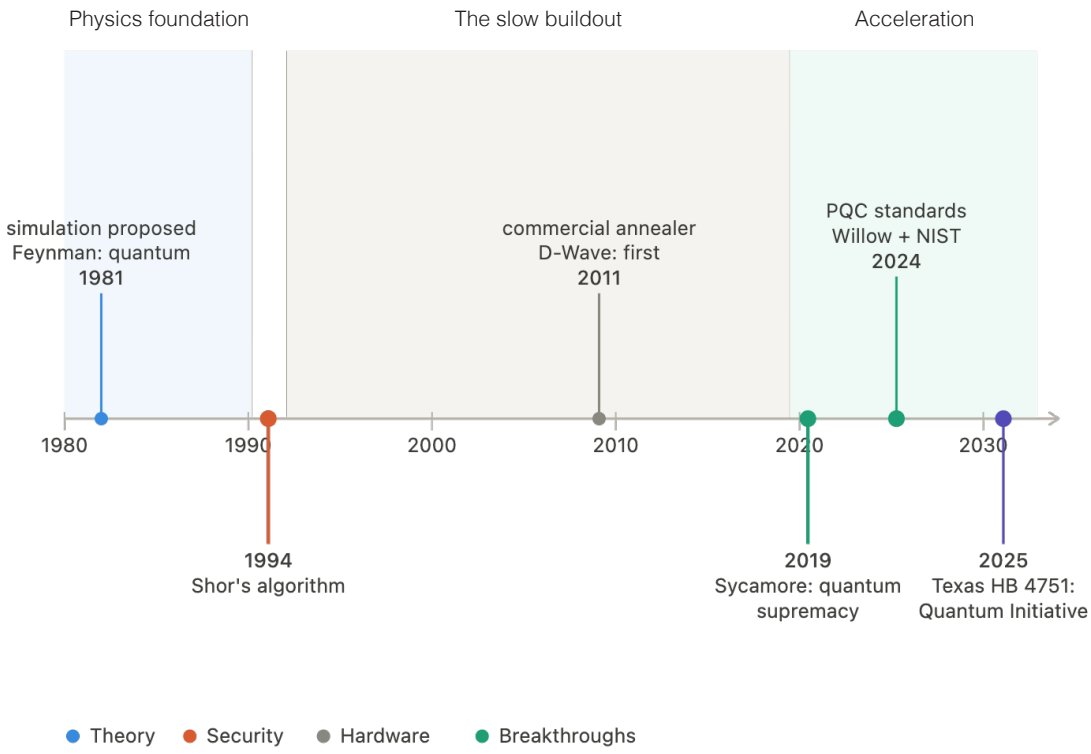
This presented a remarkable opportunity. Since nature itself was quantum, it stood to reason that the best computers to understand it would also be quantum, as they would be working from first principles of reality rather than approximations. In 1981, the famous physicist Richard Feynman arrived at exactly this conclusion and concluded that the machines we use today (which store information as ones and zeros) would fall short eventually (Feynman, 1982). **Figure 1** traces the key milestones from this point forward.

The Bombshell (1994)

Mathematician Peter Shor formally proved that the principles of quantum computation could outperform classical computers, but only in an extremely limited example: quantum computation could factor large numbers faster than any classical computer. This led to a devastating conclusion. It meant that RSA encryption, the standard which protects nearly all online banking, emails and e-commerce, could be broken.

Shor's algorithm meant that once sufficiently powerful quantum computers existed, they would be a *national security concern*.

Figure 1
Timeline of Key Quantum Computing Milestones



The Slow Buildout (1994–2019)

The theory had advanced, but in practice, quantum systems still operated at a highly limited state. Building quantum systems stable enough to function meaningfully as "computers" was out of reach, akin to trying to build calculators out of snow.

With their coherence measured in nanoseconds, they were useful only for toy experiments. This caused some funding and enthusiasm to wane as it became evident that tangible results were still far off. Yet, progress continued, however slow and unglamorous, and some of this progress would find expression in the other verticals for quantum technology: quantum sensing would begin its conceptual foundations with the Defense Advanced Research Projects Agency (DARPA), the Pentagon's advanced research arm with broad applications for biological imaging, inertial navigation, and GPS-independent positioning. Quantum networking would also begin its first steps with early experimentations of entanglement-based communications, eventually setting the theoretical foundations for what is now known as quantum key distribution.

In 2016, quantum networking was launched with China's Micius quantum satellite. Micius demonstrated that quantum signals could be distributed from orbit and was practical proof that space-based quantum networking could work. Since then, China has followed up to build a quantum communication network spanning more than 12,000 kilometers. This is an early lead in quantum networking that the United States has not yet matched.

Acceleration (2019–Present)

By 2019, breakthroughs began to accelerate. Google's Sycamore processor performed a computation in 200 seconds that would take the world's fastest classical computer at the time an estimated 10,000 years (Arute

et al., 2019). In 2024, the Google Willow chip crossed an even more fundamental threshold: decreasing error rates as more qubits were added rather than increasing the error rate. This demonstrated for the first time that quantum error correction works at scale (Acharya et al., 2024).

This was proof that the fundamental engineering challenge of reducing errors in quantum systems was possible. Funding followed these breakthroughs, with global venture capital exceeding $2 billion in 2024 alone. Cumulative equity funding in the sector has reached nearly $4 billion (McKinsey & Company, 2024).

How Quantum Computing Works: Qubits, Entanglement, and Error Correction

Qubits and Superposition

A classical computer stores information as bits: information either as 0 or 1. Conversely, a quantum bit (or "qubit") can exist in a superposition of both states simultaneously. This is the observed behavior of particles at the quantum scale and can lead to some fascinating consequences. Two qubits in superposition, then, can represent four states at once. Three qubits represent eight. The scaling is exponential and therein lies the power: 300 qubits can represent more states simultaneously than there are atoms in the observable universe.

Entanglement

When qubits become entangled (what Einstein called "spooky action at a distance"), measuring one instantly determines the state of another, regardless of physical separation or distance. Imagine if you had two balls, one in Houston and one in Dallas. If one is measured, the other will always have a corresponding measurement. This is true no matter how far apart they are.

Entanglement allows quantum computers to coordinate computations across many qubits simultaneously and is the basis for quantum networking and quantum-secured communications. Entanglement is what makes quantum technologies fundamentally different from, and more powerful than, classical systems.

Error Correction

Qubits are extraordinarily fragile. Often, they require supercooled conditions colder than those in outer space. Any number of interferences can destroy them: heat, vibration, other electronic interferences, and almost any interaction with the environment. This was (and in many ways, still is) the fundamental obstacle with quantum computing: Qubits could be assembled, but they would break in operation.

The most common solution is quantum error correction, which uses redundancy: by encoding a single "logical qubit" across many physical qubits, errors can be detected and corrected in real time. Google's Willow achievement demonstrated that this works at scale and that by adding more physical qubits, it decreased errors. As such, the hard work of getting enough qubits to do useful work remains, but this is proof that it should eventually be practical.

Competing Approaches

Unlike classical computing, which has converged on silicon transistors, quantum computing lacks a single winning technology. Six fundamentally different physical approaches are being pursued, each with distinct tradeoffs. This diversity matters for policy: Texas's primary investment should be in talent that transfers across approaches. Where hardware is acquired, it should be structured as anchor-tenant partnerships rather than long-term capital commitments tied to any single technology, since hardware can depreciate. **Table 1** summarizes these approaches.

Quantum Advantage

Quantum advantage refers to the point at which a quantum computer can solve a problem faster or more efficiently than any classical computer. This is relevant as quantum computing is not "faster classical computing" but rather a different way of harnessing nature to do computation. As such, for some problems, quantum computing promises

Table 1
Comparison of Quantum Computing Approaches

Approach	Primary Advantage	Primary Disadvantage	Scaling Bottleneck	Key Players	2026 Milestone
Superconducting	Fast gate speeds (nanoseconds)	Requires cooling to near absolute zero; massive cryogenic infrastructure	Cryogenic footprint & cross-talk between qubits	IBM, Google, Rigetti	Google Willow: Exponential error suppression. IBM: 1,000+ qubit systems.
Trapped Ions	Highest per-gate fidelity (99.9%–99.99%).	Slow gate speeds; useful computation requires millions of gates, so even 99.9% fidelity accumulates fatal errors	Ion chain scaling limits; modular networking (photonic links) unproven at scale	IonQ, Quantinuum	Quantinuum Helios: 2:1 logical qubit ratio. IonQ: barium transition, 99.9% two-qubit fidelity.
Neutral Atoms	Massive scalability; no dilution refrigerator required	Newer technology; two-qubit gate fidelity lags behind trapped ions	Two-qubit gate fidelity	QuEra, Pasqal	QuEra: 3,000-qubit continuous operation.
Photonic	Fiber-optic compatibility; room-temperature operation	Photon loss makes long computations unreliable; detector inefficiency	Photon loss & detector efficiency	PsiQuantum, Xanadu	PsiQuantum: Illinois factory commissioning.
Topological	Inherent "built-in" error protection from physics	Qubits barely proven to exist; extreme material science challenge	Extreme material science difficulty	Microsoft	Microsoft: Majorana 1 chip (8 qubits).
Annealing	Ready for commercial use today; 4,400+ qubits	Not a universal quantum computer	Limited to optimization problems; no path to general-purpose quantum computing	D-Wave	D-Wave: 4,400+ qubits; real-time logistics deployments (Volkswagen, ports).

exponentially faster solutions. For almost all other problems, it offers no demonstrable advantage.

The clearest near-term advantage is in simulating quantum systems such as molecular interactions, material properties and chemical reactions. As quantum computing researchers consulted for this paper noted, these are problems where the underlying physics itself is quantum mechanical and classical computers can only approximate what quantum computers can natively simulate.

For classical problems like route planning and grid management, on the other hand, the picture is much murkier. While some quantum approaches have produced positive results, so far no one has yet proven that quantum methods can beat the best classical methods today. This will likely happen one day, but that day could be five or 20 years away. The gap between proof-of-concept demonstrations and

commercially relevant advantage remains wide. One telling indicator is that researchers report that even well-resourced quantum computing programs do not yet have enough meaningful workloads to fully utilize existing quantum hardware. The bottleneck, as such, is not with machines, but with algorithms and applications.

How Quantum Sensing Works: Superposition, Interference, and Precision Measurement

Quantum Sensitivity

Classical sensors measure forces acting on physical objects. For example, a spring compresses, a needle deflects, or a voltage changes. Such measurements are limited by thermal noise: the random jiggling of atoms at room temperature drowns out subtle signals. Quantum sensors work differently. By using individual atoms cooled to near absolute zero, they operate entirely below that noise floor. At those temperatures, atoms behave according to quantum mechanics rather than classical physics, and quantum mechanics allows measurements of extraordinary precision to detect changes in gravity, magnetic fields, rotation, and time that would be simply invisible to any classical instrument.

Atom Interferometry

The core mechanism behind most quantum sensors is atom interferometry. When atoms are cooled and placed in superposition, they behave as waves. A quantum sensor splits a cloud of those atoms along two paths and then recombines them. The resulting interference pattern, which is the way that the two wave-paths recombine, is exquisitely sensitive to any physical differences between the two paths. For example, if gravity pulls even slightly harder on one path than the other because there is a dense rock formation or a hydrocarbon reservoir, the interference patterns shift in meaningful, measurable ways. One could think of it as the world's most sensitive ruler, and one that can detect what lies beneath the ground without drilling a single hole.

Maturity

Unlike quantum computing, quantum sensing does not require a breakthrough in either error correction or fault tolerance. Quantum gravimeters are already used commercially for oil and gas exploration and underground infrastructure mapping, while quantum atomic clocks can provide precision timing for military navigation in GPS-contested environments. The U.S. military has over $200 million invested in contracts for quantum sensing systems already (Quantum Insider, 2026).

The engineering challenge is miniaturization and cost efficiency, not fundamental scientific discovery.

How Quantum Networking Works: Entanglement, Transmission, and Key Distribution

The No-Cloning Theorem

Classical networks transmit copies of data. For example, when a message travels from Dallas to Houston over the internet, copies of that message will pass through routers, servers, and switches along the way. Quantum networks cannot work this way. A quantum state cannot be copied without being destroyed; this is a fundamental consequence of quantum mechanics known as the "no-cloning theorem." Unlike a photograph, which can be copied endlessly without affecting the original, the quantum state is destroyed by the act of reading it.

As such, any attempt to intercept a quantum transmission—which necessarily involves reading it—will disturb the signal in a way the intended recipient can detect. The security of a quantum channel, thus, is grounded in the laws of physics themselves.

Transmitting Quantum States

The primary carrier of quantum information is the photon, which is a unit of light. Entangled photon pairs are quantum states which are correlated regardless of the distance between them and can be used to establish communications channels between distant nodes. When one photon is measured, the

state of its partner is instantly determined. This is "spooky action at a distance" that underlies entanglement in quantum computing, applied in this case to communication technology. This is the mechanism behind quantum key distribution, which uses entangled photons to establish a shared encryption key between two parties and makes any eavesdropping physically detectable.

The Distance Problem

Quantum signals degrade over approximately 100 kilometers of optical fiber. Classical repeaters cannot solve this, since their form of amplification requires copying and as previously indicated, this is prohibited by the no-cloning theorem. One proposed solution is quantum repeaters, which instead of amplifying the signal, extend it by swapping it between adjacent network segments to effectively stitch together a longer channel from shorter ones.

This, however, requires quantum memory: the ability to hold a quantum state while waiting for a neighboring node to establish its own entanglement. There has been some progress on this, with recent laboratory results achieving entanglement over 10 km of fiber and quantum teleportation between photons from separate sources, but commercial quantum repeaters remain at research stage. There are workarounds, such as satellite-based transmission which is used by the Chinese Micius satellite or the use of trusted relay nodes as part of China's 12,000 km network, but the latter introduces classical vulnerabilities at each relay point, as discussed in Section III.

Quantum Key Distribution

Quantum key distribution (QKD) is the most mature quantum networking application. It uses quantum mechanics to distribute encryption keys such that any interception is detectable. QKD is distinct from post-quantum cryptography (PQC); PQC replaces vulnerable mathematical assumptions with quantum-resistant ones, while QKD provides a physical mechanism for key exchange whose security requires no mathematical assumption at all. The two can be complementary. Their applications and policy implications for Texas are addressed in Sections II and III.

II. THE PROMISE: WHAT QUANTUM CAN DO FOR TEXAS

The quantum technology stack has three legs: computing, sensing, and networking. This section focuses on practical applications: what each vertical can do for Texas, grounded in evidence rather than aspirational timelines. Claims are distinguished by evidence level:

1. **Deployed** - operational today
2. **Demonstrated** - research results published
3. **Theoretical** - scientific basis exists

Quantum Computing

Energy, Pharmaceutical, and Materials Science

Evidence Level: Demonstrated (small-scale)/ Theoretical (commercially relevant scale)

Texas is the energy capital of the world, and energy science is where quantum computing has its most scientifically credible near-term path. As Scott Aaronson of the University of Texas at Austin noted, quantum simulation (using a quantum computer to model another quantum system) is the application with the strongest case for advantage over classical machines. One image makes the case more clearly than any abstraction.

A molecule of penicillin has 41 atoms. If a classical computer were to simulate its quantum behavior precisely, it would require more computational states than there are particles in the observable universe.

This is a fundamental limit of how classical machines represent reality. Quantum computers may change this limit. This is immediately applicable to energy in the form of solar power and batteries. At the moment, developing next-generation batteries and efficient solar cells relies on expensive, slow trial-and-error

in the laboratory. Quantum algorithms offer a path to simulating the chemical pathways of electrolytes, catalysts, and photovoltaic materials with far greater precision.

In 2025, researchers used hybrid quantum-classical methods to identify surface defects in perovskite quantum dot solar cells, contributing to a record-breaking 18.3% efficiency. IonQ has demonstrated small-scale simulations of lithium-sulfur battery interactions, with IonQ targeting 2028 for commercially relevant battery modeling (although this relies on the existence of error-corrected "logical qubit" systems that do not exist).

While this landscape remains largely theoretical today and researchers can only simulate small molecules with a handful of atoms, there is a clear understanding of the gap and the bridge needed to close this gap: improved fault-tolerant technology. While the necessary hardware for this has yet to be built, the path forward is clearer than it has ever been, and research investment in this area is accelerating.

Additionally, the same simulation capabilities extend to pharmaceutical design, where modeling molecular interactions at quantum scale could revolutionize drug discovery.

Power Grid Optimization

Evidence Level: Deployed (small-scale)/Theoretical (dynamic stability modeling)

Texas's Electric Reliability Council of Texas (ERCOT) grid is increasingly complex, managing a volatile mix of energy with varying reliability standards. Outages can have devastating results, with Winter Storm Uri leaving more than 4.5 million homes without power for up to four days and resulting in the deaths of more than 240 Texans (Texas Comptroller of Public Accounts, 2021).

Avoiding this in the future is both a supply and an optimization challenge, and deciding which power plants to activate, where, and when (known as the "unit commitment" problem) is essentially an optimization challenge that grows exponentially more difficult with the system's complexity from scale to energy source mix.

This is one area where quantum hardware is already in production, although with significant caveats. For example, in Europe, D-Wave's quantum annealing systems are used by the utility company E.ON for grid partitioning and energy distribution (E.ON, 2021). However, current annealing hardware has only demonstrated unit commitment for roughly a dozen generating units.

ERCOT manages more than 1,800 market participants. Full-scale grid modeling at ERCOT's scale would require a more powerful class of quantum computer. That is the type being developed by IBM, Google, and other industry partners mentioned in this paper, and that is not yet available at the necessary scale.

Catalyst Design for Carbon Capture and Hydrogen

Evidence Level: Theoretical

Industrial chemistry presents some of the clearest "quantum-hard" problems. For example, the Haber-Bosch process for fertilizer production and carbon capture technologies are notoriously inefficient.

If quantum computers can model this faster, this could be one of the highest-value near-term verticals. Industry analyses from BCG and McKinsey identify materials science as the highest-value near-term vertical for quantum computing, with a global value approaching $100 billion by 2035 (Boston Consulting Group, 2021; McKinsey & Company, 2024).

Even a modest improvement in the catalyst efficiency for Texas's petrochemical refineries would have significant operational savings. Once again, this application remains theoretical and in need of better fault-tolerant hardware, but the economic case is so strong that it justifies workforce investment now.

Quantum Sensing

Quantum sensing is a proven technology. Of the three legs of the quantum stack, this is the one closest to generating real economic value today.

Oil and Gas Exploration and Monitoring

Evidence Level: Deployed (gravimeter instruments)/ Demonstrated (oil and gas field surveys)

Quantum sensors exploit quantum mechanical properties to achieve measurement precision that classical instruments cannot approach. Quantum gravimeters can detect minute variations in gravitational fields, revealing underground geological structures (including oil and gas deposits) at higher resolution than conventional survey equipment. This means more precise reservoir mapping, better-informed drilling decisions, and reduced exploration risk. The technology has entered commercial use: Exail's Absolute Quantum Gravimeter is deployed for subsurface monitoring, while TotalEnergies has partnered with QLM Technology to field-test quantum lidar for methane detection. That said, comparative performance data relative to traditional methods remains proprietary. However, industry investment in this, including quantum computing partnerships by ExxonMobil, BP, and Shell, suggests growing confidence in near-term returns.

Pipeline Integrity

Evidence Level: Demonstrated (pipeline leak detection, gas imaging)

Researchers at the University of Oklahoma and Oak Ridge National Laboratory are developing quantum-enhanced fiber-optic sensing systems that can detect oil and gas leaks before they cause environmental damage, with sensitivity far beyond current commercial leak detection systems (University of Oklahoma, 2021). Infleqtion, a Colorado-based quantum company that generated approximately $29 million in revenue in 2024 and holds contracts with NASA and the Department of War, has developed quantum atomic clocks with more than 100 times the precision of legacy systems (Infleqtion, 2024). These are already deployed in mission-critical environments. IonQ's acquisition of ID Quantique also gave IonQ optical gas imaging technology capable of detecting and identifying gases at distances up to 100 meters. This has immediate applications for Texas energy infrastructure. LongPath Technologies, a quantum sensing company spun out of Colorado's Elevate Quantum ecosystem, already operates laser-based methane detection systems across hundreds of thousands of acres in the Permian Basin, delivering millions in recovered gas value to Texas operators that would have otherwise been lost to undetected leaks (LongPath Technologies, n.d.; University of Colorado Boulder, 2024).

Defense and Navigation

Evidence Level: Demonstrated (GPS-denied navigation, defense contracts)/Theoretical (orbital quantum sensing payloads)

Quantum sensing has attracted significant attention for its defense applications, especially in environments which are heavily contested by electronic warfare. Quantum gyroscopes and accelerometers can provide GPS-independent navigation, which can be critical in military environments where GPS signals are denied. Such navigation systems cannot be spoofed, and thus represent a near-term application rather than a speculative one. DARPA has funded multiple quantum sensing programs; Infleqtion holds an $11 million Department of War contract for mission-critical navigation innovation. Innovation in this technology is directly relevant to Texas's military installations, such as Fort Cavazos and Joint Base San Antonio.

Quantum sensing also intersects with the space economy. The Department of Energy's Quantum-in-Space collaboration includes IonQ, Honeywell, Boeing, Axiom Space, and Infleqtion, and is developing quantum sensing payloads for orbital deployment, including Earth observation, positioning and navigation, and time synchronization. IonQ acquired satellite company Capella Space and optical communications firm Skyloom Global specifically to build space-based quantum infrastructure.

That said, no quantum sensing payload has yet flown in orbit. GPS-denied navigation using quantum gyroscopes exists as prototypes rather than in deployment. The defense investment therefore signals confidence in the science, not readiness for procurement.

Quantum Networking

Quantum networking is the ability to transmit quantum states between distant systems. It is the third pillar of quantum technology, and the least mature for near-term deployment. Its primary application is quantum key distribution, which is a form of communication that uses the laws of physics rather than mathematical complexity to secure communications. Any attempt to intercept a quantum-encrypted signal disturbs the quantum state and reveals the eavesdropper.

Ground-Based QKD

Evidence Level: Deployed (commercial QKD systems are available; JPMorgan, South Korea)/ Demonstrated (metropolitan networks)

The technology remains expensive, requires dedicated fiber-optic infrastructure, and in most applications is limited to 100 kilometers (67 miles) over fiber before signal degradation.

However, the industry has made some efforts to resolve these issues. For example, IonQ's acquisition of ID Quantique also brought a ground-based QKD appliance that integrates with existing Cisco networking infrastructure, reducing deployment complexity. Adversaries such as China appear to have made even greater strides, with the China Quantum Communication Network (CN-QCN) ostensibly operating a long-range QKD network spanning more than 12,000 kilometers, with 145 fiber nodes, satellite integration, with the ability to serve more than 800 users across banking, energy, and governmental sectors. Yet each endpoint still requires specialized hardware, and the range limitation remains. China currently extends its network through trusted relays, but as explored in Section III, the NSA specifically recommends against this approach due to the classical vulnerabilities it introduces.

Satellite-Based QKD

Evidence Level: Demonstrated (China Micius 2016, European ESA SAGA program)/Theoretical (commercial satellite QKD deployment)

Satellite-based QKD extends the range of quantum-secured communications beyond the approximately 100-kilometer limit of ground-based fiber systems. Rather than transmitting quantum states through fiber, satellites distribute entangled photons through open space, where signal loss follows different physics. China's Micius satellite demonstrated the first intercontinental QKD link in 2016, and the European Space Agency's SAGA mission is developing the next generation of space-based quantum communications infrastructure.

This technology is still limited. Satellite QKD requires line-of-sight between the satellite and ground stations, meaning that cloud cover, atmospheric turbulence, and daylight can interrupt transmission. Current systems operate most reliably at night under clear skies. Additionally, key generation rates are slow compared to classical encryption; existing systems generate keys at kilobits per second rather than the megabits or gigabits per second that modern communications demand. These constraints make satellite QKD suitable today for securing low-bandwidth, high-value communications rather than general-purpose data transmission.

In this sense, satellite QKD today resembles Morse code in the early telegraph era as a real, functional technology capable of securely transmitting high-value messages, but hardly capable of being the backbone for general communications.

Separating Signal from Noise

Quantum Washing

As quantum computing enters public awareness, a familiar (if unfortunate) pattern from other technology cycles is emerging: companies attaching

the word "quantum" to essentially classical products to inflate valuations, win government contracts, or attract investors. "Quantum AI," "quantum-enhanced analytics," and "quantum-ready solutions" are, in many cases, merely conventional software products with quantum branding. This has already led to legal consequences: for example, a major quantum computing company, Quantum Computing Inc., already faces a securities fraud class action for allegedly misrepresenting its technology and contracts.

Hype-Driven Policy Risk

Vendor roadmaps can frequently project aggressive timelines for commercial quantum applications that reflect aspirational marketing rather than scientific consensus. When these timelines drive public investment decisions, the result is misallocated capital and eventual public disillusionment that can set back legitimate quantum development by years.

When analyzing vendor case studies claiming quantum advantages in drug simulation, crash testing, and protein folding, the pattern was consistent: the actual published research uses careful language such as "benchmarks" and "proof of principle demonstrations." Ultimately, the gap between what the science says and what gets presented to investors and legislators can be significant. Outside of quantum simulation, no results today outperform the best classical methods in a fair comparison. The work is scientifically fascinating, but it does not yet constitute any broad quantum advantage.

A Legislator's Framework

When evaluating quantum claims, three questions cut through the noise:

(1) Does this require actual quantum hardware, or is it classical computing with a quantum label?

(2) Has the claimed advantage been independently demonstrated, or only on the company's own benchmarks?

(3) Does the timeline assume hardware breakthroughs that have not happened yet?

These are the same instincts legislators should apply to any emerging technology.

III. THE RISK: THE ENCRYPTION THREAT

Peter Shor's 1994 algorithm (Shor, 1994) established that a sufficiently powerful quantum computer could break the cryptographic systems running nearly all online communication. This threat is urgent enough that the National Security Agency has published its Commercial National Security Algorithm Suite 2.0 (National Security Agency, 2020), which mandates that post-quantum cryptographic standards be adopted. The National Institute of Standards and Technology (NIST), a federal agency within the Department of Commerce responsible for establishing the technical standards of American industry and national security, finalized the replacement standards in 2024 after an eight-year evaluation of 82 candidates. Texas needs to modernize, migrating our state systems to post-quantum secure methods for both practical and regulatory reasons.

How Quantum Breaks Encryption

Currently, encryption relies upon the idea that if two parties want to set up a secret channel, they first need to set up a secret code (known as a shared key) in order to communicate. This works because, similar to blending paint, the secret code is made up of the product of numbers. The key exchange functionality relies on mathematical operations that, like blending paint, are easy to perform but practically impossible to reverse. Essentially, it is easy to multiply numbers but hard to factor them.

Quantum systems with Shor's algorithm, however, break this assumption. For the first time, with a sufficiently powerful quantum computer, one can indeed unmix the paint into its individual colors, or, more specifically, factor the numbers used to create the secret code.

The solution is to use a different type of technology, such as lattice-based cryptography (a form of cryptography involving searching in high-dimensional spaces, akin to trying to find a grain of sand in a haystack), which, to the best of current knowledge, quantum computers cannot break.

Harvest Now, Decrypt Later Operations

The global internet runs through a finite number of cables, and over the past decade, multiple incidents have demonstrated the ability of nation-state actors to divert bulk encrypted traffic through their own infrastructure. This is a form of silent attack known as "harvest now, decrypt later" (HNDL), which allows mass gathering of data now for later exploitation.

Notable examples include a 2016 rerouting of Canadian internet traffic (Demchak & Shavitt, 2018) destined for South Korea into China; and in 2020, data from Google, Amazon, and over 200 other networks (Kovacs, 2020) were redirected through Russia in what appeared to be a coordinated hijacking of the internet's core routing protocol. A landmark study by the U.S. Naval War College and Tel Aviv University has painstakingly documented how China Telecom maintained points of presence in North America that allowed it to reroute and "wash" U.S. internet traffic through mainland Chinese servers over a period of years.

Although none of these incidents have been officially confirmed as HNDL operations, the pattern is consistent with bulk collection: intercept encrypted traffic, copy it, and forward it to its destination with no visible disruption. The U.S. Department of Homeland Security, the UK's National Cyber Security Centre, the European Union Agency for Cybersecurity, and the Australian Cyber Security Centre all use their official post-quantum guidance on the explicit premise that adversaries are currently collecting and storing encrypted data for future decryption.

For Texas, the implications are specific. Sites such as Fort Cavazos, Joint Base San Antonio, and Fort Bliss generate military-adjacent communications traffic that is of direct interest to foreign intelligence services. None of this data can be retroactively protected once it has been harvested. Migration to post-quantum cryptography thus must happen before a critical mass of stored intercepts can be decrypted.

Post-Quantum Cryptography

The primary solution to the quantum encryption threat is simply better math. Post-quantum cryptography refers to a new generation of encryption algorithms designed to run on existing computers while remaining mathematically intractable for both classical and quantum attackers. The leading approach is known as lattice-based cryptography, and relies on the difficulty of finding patterns in high-dimensional mathematical structures, which appears to be intractable even for quantum computers.

After an eight-year competition, the National Institute of Standards and Technology (NIST) evaluated 82 candidates. Four were selected (see **Table 2**). These standards align with the National Security Agency's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), which sets the cryptographic requirements for all national security systems and is the standard for all future federal baselines (NIST, 2024).

The Four Standards

ML-KEM (formerly CRYSTALS-Kyber)

Adopted by: Google Chrome, Apple iMessage, Signal, Cloudflare, Amazon Web Services

This is the primary replacement for the vulnerable key exchange layer. ML-KEM is built on lattice-based mathematics, or, more specifically, the hardness of the Module Learning with Errors problem. No known quantum algorithm can efficiently solve this problem. For Texas agencies, this is the single most important standard.

Table 2
NIST Post-Quantum Cryptographic Standards

Algorithm	Function	Mathematical Basis	Status
ML-KEM (Kyber)	Key Establishment	Module-Lattice	Standardized (FIPS 203)
ML-DSA (Dilithium)	Digital Signatures	Lattice-based	Standardized (FIPS 204)
SLH-DSA (SPHINCS+)	Digital Signatures	Stateless Hash-based	Standardized (FIPS 205)
HQC	Key Exchange	Hamming Quasi-Cyclic	2025 "Backup" Selection

ML-DSA (formerly CRYSTALS-Dilithium)
Adopted by: Federal agencies (per NSA CNSA 2.0 mandate), Microsoft, IBM, major cloud platforms

This is the primary standard for digital signatures, which is the mechanism that verifies the authenticity of software updates, government credentials, and legal documents. If an attacker can forge a digital signature, they can push fraudulent software updates to state systems or counterfeit official documents.

SLH-DSA (formerly SPHINCS+)
Adopted by: NSA, NIST-recommended conservative backup

This is a backup digital signature standard built on hash-based cryptography rather than lattices. It is deliberately slower and larger than ML-DSA, but relies on mathematical assumptions such that if lattice-based cryptography is ever compromised, SLH-DSA can be a fallback resort.

HQC (Hamming Quasi-Cyclic)
Adopted by: NIST, finalized March 2025. Early industry integration is underway.

Selected by NIST in March 2025 as an additional key exchange standard, HQC is built on code-based cryptography. Distinct from both lattices and hashes like SLH-DSA, its inclusion reflects a deliberate strategy of diversity: no single mathematical breakthrough should collapse the entire post-quantum framework at once.

Industry Adoption and Practical Considerations

Industry has moved quickly, as noted above. Google, Apple, Signal, and Zoom have begun implementing these standards. Amazon Web Services has deployed hybrid post-quantum key exchange across major services.

A notable approach is the cryptographic combiner approach. This method runs multiple key exchanges simultaneously: one classical, one post-quantum,

and then combines the results. Even if one of the components is broken, the other will remain secure. This is a defense-in-depth strategy, already deployed by Google and AWS and currently represents the state of the art in transitional cryptographic security.

A remaining practical concern is cryptographic overhead. Post-quantum signatures are much larger, between 24 and 40 times larger than classical ones. This can impact web performance and bandwidth. In early 2025, Google attempted to address this issue for the most latency-sensitive use case (i.e., web certificates) by introducing the Merkle Tree Certificates (MTC). This architecture reduces the data sent during each web connection to a lightweight proof. For other signature applications, such as signed documents and software updates, the larger signatures remain a practical consideration but are not fatal—they increase bandwidth, rather than computation time. A post-quantum Texas state web portal would be no slower than the current one. Signed documents would be slightly larger.

Quantum Key Distribution

As introduced in Section II, quantum key distribution (QKD) represents a fundamentally different approach to the key exchange problem. Rather than relying on mathematical complexity, QKD uses the physical properties of quantum mechanics for security.

Real deployments exist. JPMorgan Chase has piloted QKD-secured networks between data centers (J.P. Morgan, 2022), China operates the network discussed in Sections I and II and commercial QKD-as-a-service offerings are available in multiple countries. These deployments share a common profile, however: specialized, high-value, low-bandwidth links where the cost and complexity of QKD is justified by the sensitivity of the data. They are not a general-purpose communications infrastructure.

Several factors would make a broad Texas deployment premature. Cost is the most immediate barrier. QKD requires specialized hardware at approximately $100,000 per device pair (International Telecommunication Union, 2021), plus dedicated or multiplexed fiber infrastructure, while software-based PQC runs on existing infrastructure at effectively no additional cost. Range remains a hard constraint, with current systems limited to metropolitan distances. Trusted relay networks can extend this range but each relay node introduces a classical vulnerability as described below. QKD also protects only the links where it is physically installed; everything else still requires PQC, making QKD an additional cost on top of migration, rather than an alternative to it.

The NSA's 2020 advisory, reaffirmed by the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) in 2025, continues to caution against QKD due to its reliance on trusted relays and its inability to provide source authentication (National Security Agency, 2020). The field is advancing rapidly enough that hardware purchased today may be superseded before it delivers full value. Therefore, the appropriate role for QKD in Texas policy is as an experiment, not a procurement. A pilot deployment at selected facilities would allow the state to evaluate cost, performance, and feasibility in a real-world environment and publish findings to inform future legislative sessions. This would position Texas as informed and forward-looking without committing to infrastructure that may prove premature.

The Texas Gap

Federal agencies operate under Cybersecurity and Infrastructure Security Agency (CISA) mandates to prepare for a post-quantum era, and major technology companies are deploying quantum-resistant encryption protocols across their products. However, the Texas Department of Information Resources has not yet published any post-quantum cryptography guidance. This is something that Texas can, and should, address.

Closing the gap requires care. One important caution emerged from security researchers: that migration must be careful, not rushed. Cryptographic implementations are notoriously fragile, and mandating

rapid PQC migration could introduce implementation bugs that create new vulnerabilities. The recommended approach, therefore, is to experiment in controlled pilot environments before mandating broader deployment.

The researchers consulted for this paper laid out a practical three-step approach. First, use what Texas already has. AES-256 symmetric encryption is already quantum-safe and runs on every system in the state that already shares keys for internal state agency communications, encrypted storage, and VPN tunnels between known facilities.

Second, for systems that require key exchange with new parties (such as public-facing websites, interagency communications, and digital signatures), migrating to the NIST-recommended lattice-based algorithms is an excellent recommendation. This migration should begin with controlled pilot programs, thereby allowing Texas to identify and resolve implementation issues before broader deployment. Cryptographic combiner approaches, which run classical and post-quantum key exchanges simultaneously so that the system remains secure even if one component fails, offer an additional layer of protection during the transition.

Finally, for the highest-security applications where even mathematical assumptions are unacceptable, Texas Cyber Command and other relevant state entities directed by the Legislature should pilot evaluations of quantum key distribution as a long-term possibility. This should be treated as an experiment, not a deployment.

IV. THE COMPETITIVE LANDSCAPE

Federal Investment and Opportunity

The federal government has moved past the initial research initiative under President Trump with the National Quantum Initiative Act of 2018 and now has a sustained, bipartisan commitment to quantum technology as a matter of national security and economic competitiveness. For Texas legislators, three federal developments create both urgency and opportunity: the reauthorization of the National Quantum Initiative with $2.7 billion in proposed funding, new Department of Energy programs targeting energy-sector quantum applications, and binding federal post-quantum cryptography deadlines in 2030 and 2035.

The National Quantum Initiative Reauthorization

The proposed National Quantum Initiative (NQI) Reauthorization Act of 2026, introduced in January 2026 as a bipartisan effort led by Senators Cantwell and Young, would extend the federal quantum mandate through 2034 and authorize the National Science Foundation to expand its Quantum Leap Challenge Institutes from five to ten. These institutes are federally funded multidisciplinary research centers that receive $2 million to $7.5 million annually for up to six years, combining quantum research, industry partnerships, and workforce development. Five currently exist, housed at the University of Illinois, the University of Colorado, UC Berkeley, and the University of Chicago.

Currently, none are in Texas, but UT-Austin, Texas A&M, and Rice University all have research foundations to compete for the new center designations. Since federal reviewers award these institutes to states that have demonstrated sustained commitment to quantum workforce development, expanding faculty hires and research infrastructure is the demonstrated commitment that federal evaluators require. Section V outlines how Texas can position itself to capture these opportunities.

The Department of Energy Research Projects

The Department of Energy's Advanced Research Projects Agency for Energy launched the Quantum Computing for Computational Chemistry program with $37 million, targeting energy-sector simulations: catalysts, batteries, and grid optimization. The program's first-ever quantum technology award went to Infleqtion for grid optimization alongside Argonne National Laboratory (based in Lemont, IL). Related to this, Texas A&M researchers have also

Table 3
Federal Post-Quantum Cryptographic Deadlines

Deadline	Requirement	Texas Impact
August 2024	NIST finalizes first three PQC standards (FIPS 203, 204, 205). Standards ready for immediate adoption.	TX Department of Information Resources (DIR) has published no guidance for state agencies to adopt these standards.
January 2026	CISA issues formal migration checklists for critical infrastructure. CNSA 2.0 transition timeline published.	Federal agencies interfacing with Texas systems have begun migration. Texas has no matching directive.
2030	RSA-2048 and ECC-256 officially deprecated for most secure uses under NIST/CISA guidance.	ERCOT, which interfaces with DOE, NERC, and FERC-regulated systems, must begin compliance planning well before this deadline.
2035	Pre-quantum encryption algorithms (RSA, ECC) disallowed for federal and critical infrastructure use.	In effect, this would be a hard compliance deadline for any Texas system touching federal infrastructure.

begun testing quantum algorithms on synthetic ERCOT models. As the nation's largest energy-producing state and home to the largest independent grid, Texas has a direct pathway into this federal funding track (Advanced Research Projects Agency–Energy, 2024).

The 2035 Compliance Clock

The CISA compliance deadlines of 2030 and 2035 (Cybersecurity and Infrastructure Security Agency, 2023) represent binding federal mandates for Texas systems interoperating with federal infrastructure. The full security strategy is addressed in Sections III and V (see **Table 3** for the full federal post-quantum deadline structure).

Other States

At the top of the comparison (see **Table 4**), Illinois has committed approximately $840 million to quantum technology: $200 million for the Chicago Quantum Exchange, $500 million for the Illinois Quantum and Microelectronics Park on Chicago's South Side, and $140 million in co-investment with DARPA for a Quantum Proving Ground. At 1.6% of Illinois's annual general budget, it is a meaningful, if not unprecedented, level of targeted technology spending (Adams, 2026).

This has had significant results: Illinois has attracted major quantum industry partners, including IBM, IonQ, Infleqtion, and PsiQuantum, to create an emerging quantum industry cluster on Chicago's South Side. Infleqtion alone has committed $50 million and is headquartered there for its global quantum computing operations. These investments signal that Illinois has successfully positioned itself as a destination for the quantum industry, with the jobs, tax revenue, and federal grant co-investment that follow industry concentration.

Illinois's massive commitment is a gamble, one that is on a technology that is constantly changing and may not prove commercially viable for many years. Leading quantum researchers consulted for this paper noted that current quantum workloads are so limited that they can often be run on cloud-hosted systems in remote locations.

Of competing state models, Colorado's is perhaps the most instructive for Texas. Rather than committing

Table 4
State Quantum Investment Comparison

State	State Investment / Commitment	Anchor Partners & Infrastructure	Federal Footprint
Illinois	$840M (Full commitment)	PsiQuantum (IQMP), IBM, Infleqtion, DARPA QPG	2 of 5 DOE Centers; "The Bloch" Tech Hub
New York	$360M+ (State) + $20B (Private)	$300M Stony Brook Hub; $60M for 4 new regional hubs (2026 Budget)	NIST/Brookhaven DOE Center
Colorado	$114.5M (Credits/ Grants)	Elevate Quantum, Quantinuum, IonQ	NIST Boulder; Designated Tech Hub
Maryland	$27.5M (2026 Budget)	IonQ HQ, Mid-Atlantic Quantum Alliance	NSA/NIST/DOD/UMD Ecosystem
Texas	$4.8M (Seed)	UT-Austin TQI, Strangeworks	None yet

hundreds of millions to hardware and facilities, Colorado built around its existing academic anchor at the University of Colorado-Boulder and used modest state investment to leverage federal Tech Hub designation and over $2 billion in projected private capital. Texas has an equivalent—and superior—set of anchors in UT-Austin, Rice University, Texas A&M, and Texas Tech University.

Texas has already taken a first step. House Bill 4751, signed into law in June 2025, formally established the Texas Quantum Initiative, creating a seven-member advisory committee, an executive director position, and the Quantum University and Business Innovation for Texas Fund to cover computing, networking, and sensing. The Legislature now needs to allocate funding to activate what it has already created (HB 4751, 2025).

China and the Geopolitical Race

China has pursued quantum technology with a strategic urgency, though its advantages are not uniform across all three verticals. **Table 5** summarizes the strategic commitments of the leading national programs.

In quantum networking, China holds a clear lead. In 2016, China launched Micius, the world's first quantum-enabled satellite, demonstrating intercontinental quantum key distribution over 4,700 miles between Beijing and Vienna (Liao et al., 2017). By March 2025, it will have extended that reach to 8,000 miles with a quantum link to South Africa. On the ground, China operates the largest terrestrial QKD network in the world, connecting more than 150 institutions across four metropolitan areas (see **Section II**). Its 15th Five-Year Plan identifies quantum

Table 5
International Quantum Technology Strategic Commitments

Nation/Entity	2026 Strategic Commitment	Infrastructure Milestones	Strategic Narrative
China	$15B+ public investment (targeting $138B total via 15th Five-Year Plan)	12,000-km terrestrial network backbone; independent SCA cryptographic standards	"Cryptographic Sovereignty" — Building a separate, secure internet
European Union	€1B Quantum Flagship; €6B IRIS² Satellite System	EuroQCI deployment (27-nation secure link); space-to-ground QKD integration	"Strategic Autonomy" — Protecting the Union from external digital influence
United Kingdom	£1B (allocated for 2026–2030 R&D cycle)	National Quantum Computing Centre; 50+ startups under the Catapult Network	"Quantum-Enabled Economy" — Dominating high-growth tech sectors
India	$720M National Quantum Mission (operating through 2030)	Four Thematic Hubs fully operational; indigenously developed qubits	"Technological Self-Reliance" — Ending dependency on imported hardware
United States	$1B/year (NQI Reauthorization 2026 proposed)	5 existing DOE centers; 10 proposed NSF centers; NASA space-comms integration	"Lab-to-Market Engineering" — Translating theory into economic power

technology as the first of six national priority industries, backed by over $15 billion in public investment.

While China is competitive in quantum computing, it trails the United States in hardware quality and algorithmic sophistication. American companies, including Google, IBM, and Microsoft, maintain advantages in qubit quality, error correction, and commercial ecosystem maturity.

In quantum sensing, China's investments are substantial but less publicly documented, with a particular emphasis on defense applications. China has explicitly identified quantum precision measurement as a strategic priority and has cited navigation, radar, precision strike, and submarine detection as target applications. These are capabilities with direct implications for American military operations in the Pacific.

Perhaps most concerning for Western security, China has begun developing independent post-quantum cryptography standards. This is a deliberate divergence from the NIST process that the United States and its allies are following. If that divergence continues, the result could be a world divided into incompatible secure communication zones. For Texas military installations and government systems that must interoperate with federal networks, readiness to meet American standards goes beyond the technical necessity and is, in its own way, a declaration of Texas's commitment to the security architecture of the Western world.

The American response is catching up. The proposed NQI Reauthorization Act of 2026 (S. 3597, 2026) would, for the first time, formally integrate NASA into the national quantum strategy, thereby authorizing research and development in quantum satellite communications and space-based quantum sensing. This is a direct response to China's demonstrated lead in quantum satellite communications.

Incidentally, insofar as this shift places a strategic premium on states with existing space infrastructure, Texas holds advantageous assets. NASA's Johnson Space Center in Houston is the nerve center of American human spaceflight, and SpaceX's Starbase in South Texas is the most active commercial launch site in the country. Additionally, the Texas Space Commission, established by the Legislature with $150 million in funding, has been instrumental in organizing a growing network of commercial and academic partners.

V. POLICY RECOMMENDATIONS

Technology should serve humanity first, and in quantum technology, it is the humans rather than the hardware that matter most. Quantum computing requires sustained basic research, specialized talent, and patient capital in a field where no singular path to success has yet emerged and where hardware may depreciate before it delivers value. Quantum sensing, already deployable, needs targeted investment to connect its proven capabilities to Texas's industry. Quantum networking needs new ideas and courageous experiments. Each vertical requires different approaches, and the approach recommended in this paper is deliberately conservative in spending yet ambitious in outcomes.

Texas has all the ingredients to become a national—indeed, global—leader in quantum technology. Texas has a wellspring of talent from its academic institutions, and by investing to grow this network, providing an environment to rapidly iterate on ideas, and promoting cross-industry cooperation, Texas can capitalize on its strengths: leading quantum research programs, an already established and expanding quantum industry presence, and state security infrastructure, including the Texas Cyber Command.

The Why: Texas Should Lead on Quantum Technology

Texas has more at stake in the quantum race than any other state. As home to military infrastructure already being targeted by "harvest now, decrypt later" operations, adversaries are actively collecting encrypted Texas data and storing it for future decryption. The window for securing that data is closing.

This threat extends to civilian infrastructure in ways unique to Texas. ERCOT, the electric grid serving 27 million Texans, is notable in its independence; it operates as a largely isolated system with fewer interstate interconnections than almost any other regional grid in the country. This independence, while a strength of the Texas model, is also a vulnerability in the quantum security context. Any compromise of control system encryption could propagate through the entire Texas grid and lead to devastating, even lethal, consequences (Electric Reliability Council of Texas, 2026).

Since ERCOT also interfaces with federally regulated systems under the Department of Energy, NERC, and FERC, the compliance deadlines for CISA due in 2030 and 2035 apply directly. Aligning with the federal push for PQC standards will ensure that the Texas grid improves in security and stability. This has already been a critical need, but it has become even more critical in the current geopolitical environment.

Beyond the risks, however, opportunities are equally compelling, and here Texas may be in the right time and right place. Quantum sensing is the most mature of the three quantum verticals. It is already commercially deployed and requires no dramatic breakthroughs to deliver value and directly boosts Texas's oil and gas industry. The scale of what is at stake is staggering.

Oil and natural gas extraction, along with broader energy-sector support, accounted for approximately

15% of the Texas economy and $366 billion in direct economic activity in 2024 alone. Quantum gravimeters, which allow geologists to see beneath the surface without drilling, can be invaluable for locating reservoirs, mapping formations, and monitoring pipeline integrity. In an industry operating at this scale, even modest improvements in exploration precision translate into additional billions of dollars in recovered value. The state that builds this expertise will equip its energy industry with a massive advantage and protect the economic engine that funds the Texas Miracle (Texas Oil & Gas Association, 2024).

Furthermore, the strategic value of Texas's domestic energy production has never been clearer. The February 2026 disruption to oil flows through the Strait of Hormuz drove U.S. gasoline prices above $4 per gallon (35% increase in a single month) and triggered the largest coordinated emergency oil reserve release in history. This demonstrates that domestic production efficiency is not merely an economic advantage but a national security imperative.

Texas is the nation's largest domestic oil producer, responsible for almost half of total United States crude production, and is essential to protecting national independence from the vagaries of foreign supply chains. Improving Texas's oil production, then, goes beyond sound economics. It is sound national security policy.

The case for quantum computing, though different in character and less urgent in its immediate application, is arguably larger in its long-term implications. Texas's fundamentals are strong. As previously introduced, Scott Aaronson assesses Texas's theoretical quantum program and the talent in the state's universities as competitive with, if not stronger than Colorado's program, which is widely regarded as being one of the best national models. This is reflected in the research record, where in March of 2025, a team (including Aaronson) published in *Nature* the first experimental demonstration of certified randomness, which is a protocol invented at UT-Austin, with direct applications in cryptography and quantum security. Additionally, the Texas Quantum Institute already has partners with industry on quantum manufacturing.

With these advantages, Texas is well-positioned to capture the burgeoning investment, both commercial and federal, that quantum computing is attracting. With HB 4751, Texas now has the start of a framework, but the funding and specificity are not yet there. This is ripe for opportunity in the 90th Legislature.

The How: A Strategy to Activate Texas's Quantum Advantage

The following recommendations are ordered deliberately. Security actions are urgent and low-cost. They can be initiated immediately without new appropriations. Workforce and hub investments require legislative action but will deliver compounding returns over decades. Together they constitute a fiscally conservative, strategically ambitious quantum strategy suited to Texas's existing strengths and to the urgency of the moment.

Lessons from Peer States

Texas need not copy any single playbook—it can draw a distinct lesson from each state that has moved aggressively on quantum. Illinois demonstrates that concentrated capital and federal center co-location can magnetize an entire industry cluster, attracting IBM, IonQ, Infleqtion, and PsiQuantum to a single campus. Colorado illustrates capital efficiency—modest state investment in tax credits and matching grants, built around CU-Boulder and NIST, unlocked federal Tech Hub designation and catalyzed more than two billion dollars in combined investment, a return of approximately 45-to-1 on state dollars.

New Mexico offers the cautionary lesson: capital routed primarily through venture funds and tax credits, without a central operating anchor, risks flowing outward without retaining talent in-state. And Tennessee demonstrates that a single

utility-anchored testbed—EPB and IonQ's jointly funded quantum computing and networking center in Chattanooga—can establish national relevance on a modest budget, without a large, legislated package. Texas has a ready-made equivalent in ERCOT and Texas Cyber Command. The common thread is clear: tie every public dollar to a named anchor and a measurable deployment, or risk the failure mode of activity without durable in-state positioning.

Five Recommendations for a Texas Quantum Strategy

> **Recommendation 1: Direct the Texas Quantum Initiative to expand quantum research across the state's R1 universities.**

Texas leads the nation in top-tier research universities, with 16 Research 1 (R1) institutions—more than any other state. No other state begins a quantum research expansion with this much raw institutional capacity already in place. But Texas has yet to direct that capacity at a coordinated quantum research program. All researchers consulted for this paper agree that talent is the most critical investment Texas can make: a quantum computer is very important in the overall strategy, but it is only one aspect in the equation; hiring a quantum physicist today could support a program for three decades. The cost structure is asymmetric—theoretical researchers require modest startup investment, while experimental physicists require purpose-built laboratory infrastructure that is not fungible across hires, which argues for concentration over distribution and for building critical mass at a small number of deeply staffed centers rather than spreading thin grants across every campus.

The Texas Quantum Initiative (TQI), established under HB 4751, should be directed and funded to lead this expansion, leveraging existing mechanisms, the Governor's University Research Initiative (GURI) for senior faculty recruitment and the Texas University Fund (TUF) for ongoing research support—rather than creating new ones. The TQI's research investment should be organized around three priority areas: quantum computing theory and algorithms, concentrated at UT Austin's Quantum Information Center, Texas A&M's Texas Quantum Institute, and Rice University; quantum communications, networking, and cryptography, spanning UT San Antonio's College of AI, Cyber and Computing, UT Austin, UT Dallas, Texas A&M, and the University of Houston; and quantum sensing for energy, defense, and infrastructure, distributed across UT Austin, Texas A&M, Rice, UT El Paso, Texas Tech, and the University of Houston, with UT El Paso and Texas Tech prioritized for their proximity to the Permian Basin and major military installations. Faculty supported by state funds should be subject to retention commitments, ensuring Texas-trained researchers remain long enough to build programs and train the next cohort.

> **Recommendation 2: Deploy quantum computing systems at key Texas universities through anchor-tenant partnerships.**

The TQI's research expansion requires physical hardware to match. Faculty without quantum systems produce papers; faculty with quantum systems produce working capabilities, exportable reference designs, and the federal and industry co-investment that follows credible operational results. Peer-state strategies have consistently paired faculty expansion with on-premises quantum hardware deployment for exactly this reason. The Legislature should authorize the TQI, to deploy a distributed quantum computing fleet at several R1 universities—with UT Austin, Texas A&M, Rice, UT Dallas, Texas Tech, and the University of Houston as leading candidates—structured as an anchor-tenant commercial partnership with one or more quantum providers.

Recommendation 3: Build a Texas Quantum-Secure Communications Network and take immediate action to protect state systems from post-quantum threats.

The Legislature should fund the Texas Quantum-Secure Communications Network—a quantum-safe backbone anchored at Texas's leading cybersecurity research institutions and connecting Texas Cyber Command, ERCOT-adjacent grid control facilities, and military communications links at Fort Cavazos, Joint Base San Antonio, and Fort Bliss.

The cybersecurity actions must proceed immediately, in parallel with the longer-horizon network build. First, the Legislature should direct the Texas Department of Information Resources to publish post-quantum cryptographic readiness guidance and require a cryptographic inventory of state systems—an action that requires no new appropriations and addresses a mandatory compliance gap on its own timeline. Second, the Legislature should establish post-quantum cryptographic migration pilot programs at Texas Cyber Command before mandating broader statewide deployment; piloting at these sites first ensures Texas develops its own validated playbook rather than importing one. Third, every state system that interoperates with federal infrastructure faces binding CISA compliance deadlines in 2030 and 2035—the quantum-secure network and the PQC migration pilots together constitute Texas's structured response to those mandates, converting a compliance obligation into a strategic capability.

Recommendation 4: Run an annual Texas Quantum Challenge delivering university and industry pilots each year.

Real-world pilots are how Texas converts research capability into economic and security value. The TQI should administer an annual competitive quantum pilot program—structured as a public-private challenge for utilities, manufacturers, logistics operators, and defense partners—with matched funding and hands-on support. The goal is not to pick winners but to generate use cases that justify the anchor investment, give industry hands-on experience before commercial viability, and produce exportable reference solutions that Texas can license to other states and utilities. Priority verticals should reflect Texas's structural strengths: ERCOT grid optimization and critical infrastructure resilience, oil and gas reservoir mapping and methane detection, Port of Houston and border logistics, and Department of Defense navigation and positioning at Fort Cavazos and Joint Base San Antonio.

Funding should be matched between state appropriations and industry partners, with pilots coordinated alongside the Texas Grid Security Commission (SB 75) and the Texas Space Commission. Tennessee's IonQ-EPB model in Chattanooga is the proof of concept: a live testbed tied to real infrastructure establishes national relevance in ways that a research grant never can. Successful pilots should be packaged as repeatable reference architectures—code, playbooks, and training templates—that can be deployed by other states and utilities, positioning Texas as an exporter of quantum solutions, not merely a consumer of them.

Recommendation 5: Position Texas as the national quantum manufacturing and supply-chain anchor.

Texas's clearest comparative advantage in the quantum race is not in research or infrastructure—it is in manufacturing. Several peer-state quantum strategies explicitly aspire to become the primary U.S. quantum manufacturing hub, framing the ambition as doing for quantum what Arizona and Texas already do for semiconductors. Other states are actively trying to claim the role Texas already plays in the semiconductor supply chain. Texas should not cede it. The existing semiconductor manufacturing corridor—Samsung in Taylor, Texas Instruments in Sherman and Dallas, Skywater in Austin, GlobiTech, Applied Materials, and the broader CHIPS Act-funded buildout—provides the industrial base, trained workforce, and supplier ecosystem for quantum hardware

assembly, cryogenics, photonics, and control electronics that no other state can match from scratch.

The Legislature should direct the TQI to recruit a quantum manufacturing facility—hardware assembly, supplier ecosystem, or both—using the same incentive tools that brought semiconductor fabs to Texas: workforce training grants, infrastructure commitments, and coordination with the Texas Workforce Commission and the Texas Economic Development Corporation. A distributed supplier ecosystem should be cultivated across Austin, Houston, Dallas, San Antonio, and El Paso, providing precision optics, vacuum systems, cryo-electronics, and photonic components to the corridor anchor and to the broader U.S. quantum industry. This is the single most durable outcome of the entire Texas quantum strategy: it converts existing semiconductor leadership into quantum supply-chain leadership at the exact moment other states are trying to claim that role.

A Coordinated Strategy, Not Five Independent Programs

These five recommendations form a single coordinated strategy. Recommendation 1 directs the TQI to build the research pipeline across all three legs of the quantum stack. Recommendation 2 provides the quantum computing hardware that gives those researchers real systems to work on and real results to build from. Recommendation 3 builds the quantum-secure communications network that connects Texas's highest-value security workloads while driving immediate action on post-quantum cryptographic compliance. Recommendation 4 is the demand engine that converts research and infrastructure into real-world use cases—including quantum sensing applications for oil and gas, pipeline integrity, and GPS-denied navigation, the vertical with the most immediate economic and defense value to Texas. Recommendation 5 is the differentiator—the structural manufacturing advantage Texas holds that no peer state can match.

CONCLUSION

Quantum technology spans a significant expanse of applications, some of which are years from commercial viability and others of which are already being deployed today.

Quantum computing, while arguably having both the most potential and the most public attention, remains nascent. Its most disruptive near-term application is the threat it poses to encrypted communications. Quantum sensing, or the ability to use quantum systems to locate or characterize physical phenomena, can be of immediate utility to the petrochemical industries of Texas. Quantum networking remains early-stage (although geopolitical competitors have invested heavily in it), and it may someday offer a uniquely eavesdropping-immune communications system.

The opportunities and implications are world-changing. The ability for quantum systems to simulate from first principles and understand reality as it is at the quantum scale offers the ability to model materials in an unrivaled way, thus proposing benefits for medical and solar applications.

Therein lies the paper's recommendation to focus on the people: to extend grants to the present workforce, to recruit and retain top quantum researchers through targeted faculty hires, and to coordinate and leverage them to build out Texas's quantum tech concentration. Silicon Valley did not become the global leader in artificial intelligence by having the most data centers. Rather, it became a leader by consistently having the smartest people in proximity to one another. Texas already has that advantage, and its culture is well poised to draw more.

A future built around a unifying entity that brings together academia and industry and establishes connective tissue with security partners and state entities is one in which Texas has an actionable strategy for success. It is a method by which Texas can rapidly discover its strengths and weaknesses and become the gold standard for state quantum

development. In doing so, Texas will benefit not only from future discoveries but also from more widely deploying the practical knowledge it already possesses.

It also behooves Texas to understand the peril of the present moment, as the most common forms of encryption are rapidly becoming imperiled. Having a strategy to adapt and migrate to post-quantum cryptographic standards is well-advised before the chaos of migration under pressure, or worse, a genuine security disaster. Industry stands ready to assist, and Texas can experiment and discover problems before they become critical.

Although the priority should be focused on proven, low-cost interventions such as cryptographic combiner techniques, there exists the very real opportunity to execute quantum networking experiments and, as noted, acquire invaluable scientific knowledge.

Ultimately, given the vast spending by other states and by American geopolitical competitors, the signal is clear: this is a field of escalating importance in the mid-term and of immense importance in the long-term. Disengagement is unwise and would cede leadership in a transformative field. However, undisciplined spending would be equally unwise and risk misallocating resources in a way that would neglect opportunities for compounding benefit. This paper points to a clearer path: an evidence-based, targeted investment in talent and standards to secure Texas's leadership in the quantum era.

The same value-based approach that built the Texas Miracle will also build Texas's future in the quantum frontier. ■

REFERENCES

Aaronson, S. (2025, November 12). *IBM's big bet on new quantum processors.* Semafor. https://www.semafor.com/article/11/12/2025/ibms-big-bet-on-new-quantum-processors

Acharya, R., et al. (2024). Quantum error correction below the surface code threshold. *Nature, 638*(8041), 920–926. https://doi.org/10.1038/s41586-024-08449-y

Adams, A. (2026, January 27). *How much public and private money is powering Chicago's quantum push?* Illinois Answers Project. https://illinoisanswers.org/2026/01/27/how-much-public-and-private-money-is-powering-chicagos-quantum-push/

Advanced Research Projects Agency–Energy. (2024). *Quantum computing for computational chemistry (QC3) program*. U.S. Department of Energy. https://arpa-e.energy.gov/technologies/programs/qc3

Arute, F., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Boston Consulting Group. (2021). *The next decade in quantum computing: How to play.* https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play

Cybersecurity and Infrastructure Security Agency. (2023, August). *Quantum-readiness: Migration to post-quantum cryptography*. https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

Demchak, C. C., & Shavitt, Y. (2018). China's maxim – leave no access point unexploited: The hidden story of China Telecom's BGP hijacking. *Military Cyber Affairs, 3*(1). https://doi.org/10.5038/2378-0789.3.1.1050

E.ON. (2021, March 11). *E.ON and D-Wave announce collaboration on quantum computing.* https://www.dwavequantum.com/resources/application/optimizing-the-renewable-energy-grid-with-quantum-computing/

Electric Reliability Council of Texas. (2026, February). *ERCOT fact sheet.* https://www.ercot.com/about/profile

Elevate Quantum. (2024, July 2). *Elevate Quantum awarded $127 million to secure U.S. leadership in quantum technology.* https://www.elevatequantum.org/elevate-quantum-awarded-127-million-to-secure-us-leadership-in-quantum-technology/

Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics, 21*(6–7), 467–488. https://doi.org/10.1007/BF02650179

Google Security. (2026, February). *Merkle tree certificates for TLS.* Google Security Blog. https://security.googleblog.com/2026/02/cultivating-robust-and-efficient.html

HB 4751. Texas Quantum Initiative Act. 89th Texas Legislature. Regular Session. (2025). https://capitol.texas.gov/BillLookup/History.aspx?LegSess=89R&Bill=HB4751

Infleqtion. (2024, January 31). *Infleqtion achieves record growth in 2023.* https://infleqtion.com/infleqtion-enters-2023-on-heels-of-milestone-year/

International Telecommunication Union. (2021). *Technical report on QIT4N use cases: Quantum key distribution network*. https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-QIT4N-2021-D2.2-PDF-E.pdf

J.P. Morgan. (2022, February 15). *J.P. Morgan, Toshiba and Ciena demonstrate first quantum key distribution network.* https://www.jpmorgan.com/technology/technology-blog/jpmc-toshiba-ciena-build-first-quantum-key-distribution-network-critical-blockchain-application

Kovacs, E. (2020, April 6). *Russian telco hijacked internet traffic of major networks.* SecurityWeek. https://www.securityweek.com/russian-telco-hijacked-internet-traffic-major-networks-accident-or-malicious-action/

Liao, S.-K., et al. (2017). Satellite-to-ground quantum key distribution. *Nature, 549*, 43–47. https://doi.org/10.1038/nature23655

LongPath Technologies. (n.d.). *Cutting-edge emissions monitoring solutions.* https://www.longpathtech.com/

McKinsey & Company. (2024, April 24). *McKinsey quantum technology monitor.* https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage

National Institute of Standards and Technology. (2024, August). *Post-quantum cryptography standards: FIPS 203, 204, 205.* U.S. Department of Commerce. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

National Institute of Standards and Technology. (2024, November). *NIST IR 8547: Transition to post-quantum cryptography standards.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8547.ipd

National Institute of Standards and Technology. (2025, March). *NIST selects HQC as fifth algorithm for post-quantum encryption*. U.S. Department of Commerce. https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-algorithm-post-quantum-encryption

National Quantum Initiative Reauthorization Act of 2026, S. 3597, 119th Cong. (2026). https://www.congress.gov/bill/119th-congress/senate-bill/3597

National Security Agency. (2020). *Quantum key distribution (QKD) and quantum cryptography (QC)* [Advisory]. National Security Agency. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Quantum Insider. (2026, March 2). *Understanding quantum sensing and its industrial potential*. The Quantum Insider. https://thequantuminsider.com/2026/03/02/understanding-quantum-sensing-industrial-potential/

SB 2066. 89th Texas Legislature. Regular Session. (2025). https://capitol.texas.gov/BillLookup/History.aspx?LegSess=89R&Bill=SB2066

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science,* 124–134. https://doi.org/10.1109/SFCS.1994.365700

Texas Comptroller of Public Accounts. (2021, October). *Winter Storm Uri 2021*. Fiscal Notes. https://comptroller.texas.gov/economy/fiscal-notes/archive/2021/oct/winter-storm-impact.php

Texas Oil & Gas Association. (2024). *TXOGA annual energy & economic impact report.* https://www.txoga.org/txoga-annual-energy-economic-impact-report/

U.S. Department of Energy. (2025, November). *Department of Energy allocates $625 million for national quantum research centers.* https://www.nextgov.com/emerging-tech/2025/11/energy-allocates-625m-national-labs-quantum-research/409300/

University of Colorado Boulder. (2024, October 25). *Spinout LongPath Technologies to expand methane detection with $162M DOE loan.* https://www.colorado.edu/today/2024/10/25/spinout-longpath-technologies-expand-methane-detection-162m-doe-loan

University of Oklahoma. (2021). *Researchers aim to improve oil, gas leak detection with quantum-enhanced sensing*. https://www.ou.edu/research-norman/news-events/2021/researchers-aim-to-improve-oil-gas-leak-detection-with-quantum-enhanced-sensing

ABOUT THE AUTHOR

Shon Pan is a policy writer and technologist focused on human thriving amid technological change. He co-authored "What Christians Should Know About AI" with Dr. Stefan Jungmichel of the Biola University AI Lab, funded by the Future of Life Institute. He has built cross-ideological relationships spanning conservative organizations and AI safety organizations, with policy writing focused on prioritizing human dignity and safety. He brings over twenty years of technical program management in banking infrastructure and cybersecurity, including leadership roles at Bank of America and Toyota. He is based in Dallas, Texas as a father of two sons.

Texas Public
POLICY FOUNDATION

901 Congress Avenue | Austin, Texas 78701 | (512) 472-2700 | www.TexasPolicy.com