Introduction to Quantum for Government and National Security

Understanding the Technology, the Reality, and What to Do Now

SecureFi Institute

While every precaution has been taken in the preparation of this book, the publisher assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

Introduction to Quantum for Government and National Security

Understanding the Technology, the Reality, and What to Do Now

First edition. March 2026.

SecureFi Institute

Executive Summary

Quantum computing is emerging as a new class of technology capable of solving certain problems that are impractical or impossible for today's classical computers. While large-scale, commercially viable quantum systems are still years away, the pace of research, investment, and early-stage capability development is accelerating.

Quantum computing will not replace classical computing. Instead, it will complement existing high-performance computing and artificial intelligence systems, enabling new approaches to complex challenges in areas such as cryptography, materials science, logistics, and data analysis.

The most immediate implication is in cybersecurity. Future quantum systems are expected to break widely used public key cryptographic methods, creating long-term risk for sensitive data. Adversaries can capture encrypted information today and decrypt it in the future as quantum capabilities mature. Organizations must begin transitioning to post-quantum cryptographic standards now to ensure long-term security and resilience.

At the same time, significant technical challenges remain. Reliable quantum systems require advances in error correction, scalable hardware, and the development of new algorithms. These constraints mean that quantum advantage for most real-world applications has not yet been achieved.

This document provides a practical introduction to quantum computing for government and national security leaders. It focuses on what quantum is, where it matters, the current reality of the technology, and the actions organizations should take today to prepare for its impact. The transition timeline remains uncertain, but preparation timelines are not.

Why Quantum Matters for the U.S. Government

Quantum computing is not simply a new technology. It represents a strategic capability with implications for national security, economic competitiveness, and scientific leadership.

The United States government has historically led in the development of advanced computing, from early supercomputers to today's high-performance computing environments. Quantum computing is viewed as the next phase in this evolution.

Several factors make quantum particularly relevant for government organizations.

First, national security. Future quantum systems have the potential to disrupt current cryptographic standards, impacting secure communications, intelligence systems, and critical infrastructure protection. Preparing for this transition is a matter of long-term security planning.

Second, scientific leadership. Agencies such as the Department of Energy rely on advanced computing to support research in energy, materials, climate, and physics. Quantum computing offers the potential to model complex systems that are beyond the reach of classical methods.

Third, economic competitiveness. Global investment in quantum technologies is increasing, with significant activity across the United States, Europe, and Asia. Maintaining leadership in this area is closely tied to innovation, workforce development, and industrial capability.

Finally, infrastructure evolution. Quantum computing is expected to integrate with existing high-performance computing and artificial intelligence systems, creating hybrid environments that expand what is computationally possible.

For government leaders, the importance of quantum is not immediate deployment, but strategic awareness and early preparation aligned to long-term mission needs.

The key takeaway is that quantum computing is a strategic capability with long-term implications for national security, scientific leadership, and economic competitiveness, requiring early awareness and preparation across government.

What Quantum Is (and Isn't)

Quantum computing is an approach to processing information based on the principles of quantum mechanics. Unlike traditional computing, which relies on binary bits that represent either a zero or a one, quantum computing uses quantum bits, or qubits, which can represent multiple states at the same time.

Figure 1. Classical, Quantum, and Hybrid Computing Models

This figure illustrates the relationship between classical computing, quantum computing, and hybrid computing environments. Classical systems support many workloads, while quantum systems are introduced for specific problem types. Hybrid models integrate these capabilities to address complex challenges more effectively.

This difference is not simply an improvement in speed. It represents a fundamentally different way of solving certain types of problems. Classical computers process information step by step, even when operating at very high speeds. Quantum systems approach problems by structuring them in ways that allow many possible outcomes to be evaluated through probability and interference.

It is important to understand that quantum computing is not a replacement for classical computing. Everyday applications such as word processing, databases, enterprise systems, and most analytics will continue to rely on classical architectures. High-performance computing systems will remain essential and will work alongside quantum systems in hybrid environments.

Quantum computing is best suited for specific categories of problems that involve complex interactions, large numbers of variables, or mathematical structures that are difficult to model using traditional methods. These include areas such as cryptography, molecular simulation, advanced optimization, and certain types of pattern analysis.

At the same time, quantum computing remains an emerging capability. Today's systems are limited in scale, sensitive to environmental conditions, and prone to error. Most current quantum applications are experimental, and practical, large-scale use is still in development.

The key takeaway is simple. Quantum computing is not about doing everything faster. It is about solving certain problems differently. Organizations do not need to replace their current systems, but they do need to understand where quantum may change what is possible in the future.

How Quantum Works (Plain English)

Quantum computing is based on a small number of principles that behave differently from the physics we experience in everyday life. While the underlying science is complex, the core ideas can be understood at a conceptual level.

The first concept is superposition. A classical bit can only exist as a zero or a one. A qubit can exist in a combination of both at the same time. This allows quantum systems to represent many possible states simultaneously. Instead of evaluating one option at a time, the system can structure a problem so that multiple possibilities are considered within a single computational process.

The second concept is entanglement. Qubits can become linked in such a way that the state of one is directly related to the state of another, regardless of distance. This relationship allows quantum systems to coordinate information across multiple qubits, creating more complex and connected computational structures than classical systems can achieve.

The third concept is interference. Quantum systems use wave-like behavior to amplify correct outcomes and cancel out incorrect ones. As a computation progresses, different possibilities interact with each other. Some are reinforced, while others are reduced. The final result is not determined by checking every path, but by shaping the probability of outcomes so that the correct answer is more likely to emerge.

The final concept is decoherence. Quantum states are fragile and can be disrupted by even small interactions with their environment. When this happens, the system loses its quantum properties and behaves more like a classical system. This instability is one of the primary technical challenges in building reliable quantum computers.

Together, these principles enable a different model of computation. Instead of processing information sequentially, quantum systems structure problems in ways that allow the solution to emerge from the interaction of many possibilities.

The key takeaway is that quantum computing does not work by trying every option faster. It works by organizing problems so that the correct answer becomes more likely through the physics of the system itself.

Where Quantum Matters

Quantum computing is not intended for general-purpose use. Its value lies in solving specific types of problems that are difficult or impractical for classical systems. For government and national security organizations, several areas stand out as particularly relevant.

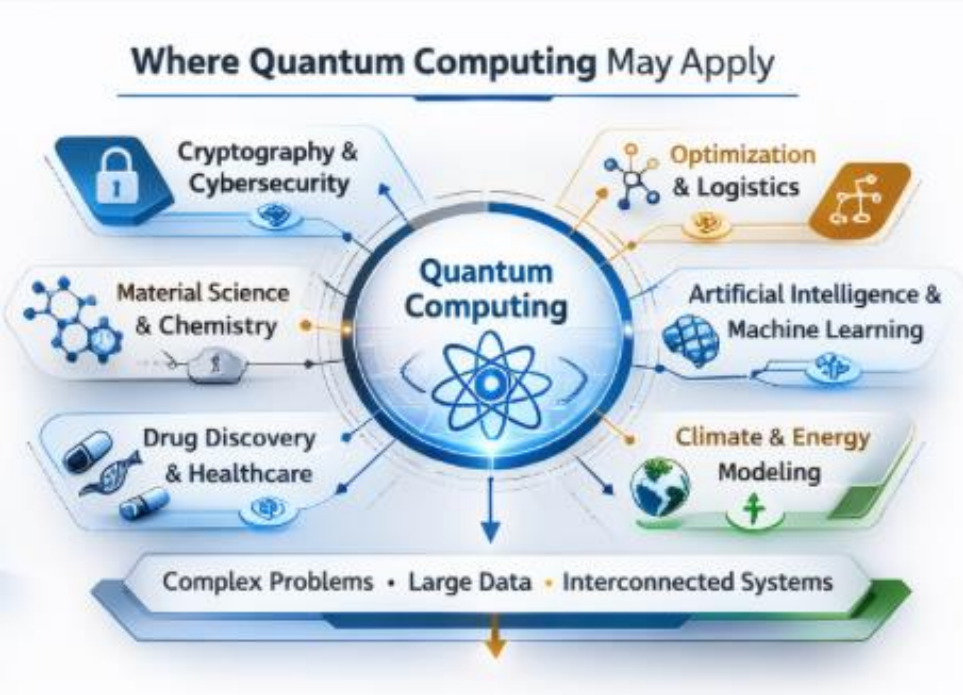

Figure 2. Representative Areas Where Quantum Computing May Apply

Quantum computing is expected to impact specific domains that involve complex relationships, large datasets, or combinatorial challenges. These include cryptography, optimization, material science, and advanced data analysis. Most applications remain in development and will evolve alongside classical systems.

Cybersecurity is the most immediate and widely discussed impact. Many current encryption methods rely on mathematical problems that are difficult for classical computers to solve but are expected to be vulnerable to future quantum systems. This creates a long-term risk to sensitive data, communications, and critical infrastructure. At the same time, quantum technologies are also enabling new approaches to secure communication, including quantum-resistant cryptography and quantum key distribution.

Materials science and energy research are also key areas of focus. Quantum systems are well suited to modeling the behavior of molecules and materials at the atomic level. This capability could accelerate the discovery of new materials for energy storage, advanced manufacturing, and defense applications. For government agencies involved in energy, science, and national laboratories, this represents a significant opportunity.

Logistics and optimization present another important use case. Many operational challenges involve coordinating large numbers of variables under constraints, such as supply chains, transportation, and mission planning. Quantum approaches may provide new ways to identify more efficient solutions in complex environments where classical methods struggle to scale.

Intelligence and data analysis may also benefit from quantum techniques. While quantum computing is not a replacement for artificial intelligence, it may enhance certain types of pattern recognition and probabilistic analysis. This could support areas such as signals intelligence, anomaly detection, and complex data correlation.

It is important to recognize that not every problem requires quantum computing. In many cases, classical systems, including high-performance computing and AI, remain the most effective tools. The role of quantum is to complement these capabilities, not replace them.

In most cases, quantum computing will be introduced alongside existing systems rather than as a standalone capability.

The key takeaway is that quantum computing should be viewed as a targeted capability. Its impact will be significant in specific domains, particularly where complexity exceeds the practical limits of classical approaches.

Additional Perspective on Hybrid Computing

In many cases, quantum computing will not replace existing methods but will enhance them. For example, a classical system may narrow down a problem space, while a quantum system explores complex interactions within that space.

This combined approach is already being explored in research environments and is expected to define how quantum capabilities are used in practice.

For government organizations, the value of quantum will emerge gradually through integration with existing systems rather than through immediate, standalone deployment.

High-Performance Computing as the Foundation

Figure 3. High-Performance Computing as the Foundation for Advanced Computing

High-performance computing systems provide the foundation for many government missions, including defense modeling, weather forecasting, and scientific research. Quantum computing is expected to complement these systems as part of an integrated computing environment.

Before quantum computing can be understood, it is important to recognize the role of high-performance computing across the federal government.

High-performance computing systems are already central to national missions. They support climate modeling, nuclear security, intelligence analysis, engineering simulation, and advanced research across multiple agencies.

The Department of Energy is the global leader in this space. National laboratories such as Oak Ridge, Argonne, and Lawrence Livermore operate some of the most powerful supercomputers in the world. Systems such as Frontier and Aurora are designed to perform at exascale levels, enabling unprecedented computational capability.

Other agencies also rely heavily on high-performance computing.

Across the federal government, high-performance computing supports mission-critical functions including defense modeling, aerospace design, weather prediction, intelligence analysis, and scientific research. Agencies such as the Department of Defense, NASA, NOAA, and the intelligence community rely on these systems for daily operations.

These systems represent decades of investment and are essential to current operations. Quantum computing is not a replacement for these capabilities. It is an extension.

The future of advanced computing is expected to be hybrid, combining classical high-performance systems, artificial intelligence, and quantum capabilities into integrated environments.

Understanding this foundation is critical. Quantum computing will build on what already exists, not replace it.

The key takeaway is that quantum computing builds on decades of investment in high-performance computing and will be integrated into existing environments rather than replacing them.

Department of Energy and Quantum Integration

The integration of quantum computing into national infrastructure is already underway across the federal government. The Department of Energy has emerged as a central leader in this effort, building on decades of investment in high-performance computing and scientific research. Its approach provides a practical model for how quantum capabilities can be introduced into existing environments.

Figure 4. Federal Leadership in Advanced Computing and Quantum Integration

The Department of Energy and national laboratories are leading efforts to integrate quantum computing with existing high-performance computing environments. This ecosystem supports research, experimentation, and early-stage deployment of hybrid computing capabilities across federal missions.

The Department of Energy is leading the effort to integrate quantum computing into national research and computing environments. Through its national laboratories and research programs, DOE has established a coordinated approach that brings together quantum research, high-performance computing, and applied science.

Initiatives such as the National Quantum Information Science Research Centers and investments through the Office of Science are advancing both quantum hardware and quantum algorithms. These efforts are closely aligned with existing supercomputing infrastructure.

A key focus is the development of hybrid computing environments where quantum systems and classical supercomputers work together. In this model, quantum processors are used for specific tasks where they provide advantage, while classical systems handle the majority of computation.

DOE laboratories are already exploring how quantum systems can be integrated into existing workflows, including materials discovery, energy systems, and complex simulations.

This approach reflects a broader reality. Quantum computing will not emerge as a standalone capability. It will be incorporated into existing computing ecosystems, led by organizations that already operate at the forefront of high-performance computing.

For government leaders, DOE provides a model for how to approach quantum. Start with strong classical foundations, integrate emerging capabilities, and focus on mission-driven applications.

The key takeaway is that quantum computing will be integrated into existing computing environments, not deployed as a standalone capability, with the Department of Energy leading this hybrid approach.

Who Is Investing in Quantum Today

Quantum computing is not confined to research laboratories. It is the focus of sustained investment across major technology companies, government agencies, and a growing ecosystem of specialized startups. This level of activity reflects long-term strategic interest rather than short-term maturity.

Several leading organizations are shaping the direction of quantum computing.

IBM has been one of the most consistent leaders in quantum development. The company has built a global quantum network, provides cloud access to quantum systems, and continues to advance both hardware and software through its Qiskit platform. IBM's roadmap includes scaling toward fault-tolerant quantum systems over the coming decade.

Google has focused on advancing quantum hardware and demonstrating key technical milestones. Its Quantum AI division has made progress in areas such as quantum error correction and processor development, highlighting the path toward more stable and scalable systems.

Microsoft is pursuing a differentiated approach through topological qubits while building a broader ecosystem through its Azure Quantum platform. The company is focused on creating a full-stack environment that integrates quantum with classical cloud computing and artificial intelligence.

Amazon is investing through its Amazon Braket service, which provides access to multiple quantum hardware platforms via the cloud. This approach emphasizes flexibility and experimentation, allowing users to explore different quantum technologies without committing to a single architecture.

In addition to large technology companies, several specialized firms are advancing quantum capabilities.

IonQ is developing trapped ion quantum systems known for stability and precision.
Rigetti Computing is focused on superconducting qubit architectures and hybrid quantum-classical computing.
D-Wave is advancing quantum annealing systems designed for optimization problems.

Government investment is also significant. The United States has committed substantial funding through initiatives such as the National Quantum Initiative Act, with participation from agencies including the Department of Energy, the National Science Foundation, the Department of Defense, and the National Institute of Standards and Technology.

Internationally, countries across Europe, Asia, and the Middle East are making sustained investments in quantum computing, recognizing it as a strategic technology with long-term implications. Nations such as Israel have developed strong quantum ecosystems supported by government funding, academic research, and startup innovation, particularly in areas such as cybersecurity and quantum software.

Companies such as IQM, a European quantum computing firm, are focused on building scalable quantum hardware and partnering with national laboratories and research institutions to deploy quantum systems. These efforts are contributing to the development of hybrid computing environments and expanding access to early-stage quantum capabilities.

This level of investment signals long-term commitment rather than immediate maturity. No single approach has emerged as dominant, reinforcing the importance of flexibility and continued evaluation.

For government organizations, this level of investment provides both opportunity and caution. While access to emerging capabilities is expanding through cloud platforms and partnerships, the diversity of approaches and rapid pace of change reinforce the importance of measured engagement and informed decision making.

The key takeaway is that sustained global investment across industry and government reflects long-term strategic importance, while the diversity of approaches reinforces the need for flexibility and continued evaluation.

Quantum Computing Reality Check

Quantum computing is advancing, but it is still in the early stages of development. While progress in hardware, software, and investment are accelerating, practical, large-scale quantum systems capable of delivering consistent commercial or operational advantage are not yet available.

Understanding the current reality is essential for making informed decisions. Recent insights from leading research institutions highlight several key signals that define where quantum stands today and what is required to move it forward.

First, more quantum algorithms are needed. While foundational algorithms exist, including those with implications for cryptography and optimization, many real-world problems do not yet have clearly defined quantum solutions. Advancing quantum computing will require continued exploration of how to apply it effectively across different domains.

Second, classical computing remains essential. High-performance computing and artificial intelligence continue to deliver most of the computational capability today. Quantum systems are expected to operate alongside these technologies, forming hybrid environments rather than replacing existing infrastructure.

Third, the transition to post-quantum cryptography must begin now. Even though a cryptographically relevant quantum computer has not yet been realized, the risk to current encryption is long-term. Sensitive data captured today could be exposed in the future as quantum capabilities mature. Preparing for this transition requires time, planning, and coordination across systems and organizations.

Fourth, quantum error correction is the gating factor for scale. Today's qubits are fragile and prone to error, limiting the size and reliability of quantum systems. Significant advances in error correction are required before quantum computers can perform the large number of operations needed for practical applications.

Taken together, these signals point to a clear conclusion. Quantum computing is progressing from scientific research toward engineering reality, but it has not yet reached broad operational use.

The key takeaway is that this is not a moment for either dismissal or overreaction. The risk is not that quantum will arrive suddenly and replace existing systems. The risk is that organizations will underestimate the time required to prepare and will be forced to respond too late.

What Leaders Should Do Now

Quantum computing does not require immediate adoption, but it does require immediate awareness and preparation. The organizations that benefit most will not be those that move first, but those that prepare early and act deliberately.

The following actions provide a practical starting point for government and national security leaders.

Begin planning for post-quantum cryptography.
The transition to quantum-resistant encryption is a long-term effort that will require coordination across systems, vendors, and policies. Organizations should begin assessing where current cryptographic methods are used, understanding emerging standards, and developing transition strategies aligned to guidance from national standards bodies. This is the most immediate and actionable step.

Build awareness across leadership and technical teams.
Quantum computing introduces concepts that differ from traditional approaches to technology. Leaders do not need deep technical expertise, but they do need a working understanding of what quantum is, where it applies, and what it does not change. Establishing a common baseline of knowledge will improve decision making and reduce confusion as the field evolves.

Establish test and evaluation environments.
Rather than waiting for fully mature systems, organizations should consider how to evaluate quantum technologies in controlled environments. This may include partnerships with research institutions, access to cloud-based quantum platforms, or participation in shared computing environments. Early exposure supports better long-term planning and reduces risk.

Monitor the ecosystem without overcommitting.
The quantum landscape is evolving rapidly, with significant activity across industry, academia, and government. Organizations should track developments in hardware, software, and standards, while avoiding premature commitments to specific vendors or technologies. Flexibility is important in an environment that is still changing.

Integrate quantum into broader technology strategy.
Quantum computing should not be viewed in isolation. Its future impact will be closely tied to advancements in high-performance computing, artificial intelligence, and data infrastructure. Planning efforts should consider how these capabilities will work together rather than treating quantum as a standalone initiative.

The key takeaway is that preparation can begin now without large investment or disruption. Awareness, planning, and measured engagement will position organizations to respond effectively as quantum capabilities mature.

Key Terms (Simple Definitions)

The following terms provide a simple reference for commonly used concepts in quantum computing. These definitions are intended to support general understanding and do not require a technical background.

Qubit
The basic unit of quantum information. Unlike a classical bit, which represents either a zero or a one, a qubit can represent a combination of both states at the same time.

Superposition
The ability of a qubit to exist in multiple states simultaneously. This allows quantum systems to represent many possible outcomes within a single computation.

Entanglement
A property where two or more qubits become linked, such that the state of one is directly related to the state of another. This enables coordination across qubits in ways not possible in classical systems.

Interference
The process by which quantum systems amplify correct outcomes and reduce incorrect ones. This allows the system to increase the probability of arriving at a useful result.

Decoherence
The loss of quantum behavior due to interaction with the environment. Decoherence introduces errors and is one of the primary challenges in building reliable quantum systems.

Quantum Algorithm
A set of instructions designed to run on a quantum computer. These algorithms are structured differently from classical algorithms and are still an active area of research.

Quantum Advantage
The point at which a quantum computer can solve a problem more effectively than the best known classical methods. This has not yet been broadly achieved for most real-world applications.

Post-Quantum Cryptography (PQC)
Cryptographic methods designed to remain secure against future quantum attacks. These methods are being standardized to replace current vulnerable encryption systems.

Hybrid Computing
An approach that combines classical computing, artificial intelligence, and quantum computing to solve problems more effectively than any single system alone.

High-Performance Computing (HPC)
Advanced computing systems capable of performing large-scale calculations at very high speeds. HPC systems are widely used across government and will remain essential alongside quantum computing.

Common Misconceptions

As interest in quantum computing grows, several common misconceptions can create confusion or lead to incorrect assumptions. Clarifying these points helps establish a more accurate understanding of the technology.

Quantum computing will replace classical computing
This is not expected to occur. Quantum systems are designed for specific types of problems and will operate alongside classical systems rather than replacing them.

Quantum computers are simply faster computers
Quantum computing is not just about speed. It represents a different way of structuring and solving certain problems, particularly those involving complex interactions and large numbers of variables.

Quantum computing is ready for widespread use today
Current quantum systems are still in early stages. While progress is being made, large-scale, reliable quantum computing has not yet been achieved.

All encryption will be broken immediately by quantum computers
While quantum computing poses a future risk to current cryptographic systems, this capability does not yet exist at scale. The concern is long-term, which is why early preparation is important.

Quantum computing only matters for scientists and researchers
Quantum computing has implications for cybersecurity, national security, logistics, and infrastructure. Leaders across government and industry should understand its potential impact.

There is a single approach to building quantum computers
Multiple technologies are being developed, including superconducting qubits, trapped ions, and other approaches. No single method has emerged as dominant.

Organizations need to invest heavily in quantum computing now
Immediate large-scale investment is not required. The priority is awareness, planning, and measured engagement as the technology continues to mature.

How to Engage

Organizations do not need to make immediate investments in quantum computing, but they should begin building awareness, assessing impact, and preparing for long-term change. Engagement can begin with practical, low-risk steps that support informed decision making.

Awareness and Education
Establish a baseline understanding of quantum computing across leadership and technical teams. This includes executive briefings, foundational training, and structured discussions on how quantum may impact mission areas.

Assessment and Planning
Evaluate where quantum computing may affect current systems, particularly in areas such as cryptography, data protection, and long-lifecycle infrastructure. Begin developing transition plans aligned with emerging standards and organizational priorities.

Workshops and Strategy Sessions
Facilitate focused discussions that bring together leadership, technical experts, and stakeholders to explore implications, identify risks, and define next steps. These sessions help align perspectives and establish a coordinated approach.

Test and Evaluation Environments
Explore access to quantum capabilities through cloud platforms, research partnerships, or shared computing environments. Early exposure supports better understanding without requiring significant investment.

Ongoing Advisory and Support
As the quantum landscape evolves, organizations may benefit from continued guidance to monitor developments, interpret emerging standards, and refine strategies over time.

Engagement should be measured, informed, and aligned to mission needs. The objective is not to move quickly, but to move deliberately with a clear understanding of the evolving landscape.

About SecureFi Institute

SecureFi Institute is an independent, non-partisan initiative focused on advancing awareness, readiness, and practical understanding of emerging technologies across government and industry.

The Institute provides research, education, and advisory support in areas including quantum computing, post-quantum cryptography, artificial intelligence, and advanced computing infrastructure. Its focus is on helping organizations navigate complex technology transitions with clarity, context, and informed decision making.

SecureFi Institute works with leaders, technical teams, and organizations to bridge the gap between emerging capabilities and real-world application. This includes developing foundational knowledge, supporting strategic planning, and enabling responsible adoption of new technologies.

The Institute's approach emphasizes practical guidance over technical complexity, ensuring that decision makers can understand not only what technologies are emerging, but what actions are required in response.

For more information or to engage with SecureFi Institute, visit SecureFi.com or contact the Institute directly.

Closing Perspective

Quantum computing will not arrive all at once. It will evolve over time through research, engineering progress, and practical experimentation before reaching broad operational use.

For government and national security organizations, the importance of quantum is not defined by when it becomes fully mature, but by how early preparation begins. Transitioning to new cryptographic standards, integrating with existing computing environments, and building internal understanding will all take time.

Organizations that start now will have the advantage of measured adoption, informed decision making, and reduced risk. Those that wait may find themselves reacting to change rather than shaping it.

Quantum computing is part of a broader shift in advanced computing that includes high-performance systems and artificial intelligence. Together, these capabilities will shape how complex problems are addressed in the years ahead.

The opportunity is not simply to adopt a new technology, but to build readiness before it is required.

Figures and Analytical Models

All figures, diagrams, and analytical models presented in this research brief were developed by SecureFi Institute as part of its research on emerging computing architectures and cybersecurity implications.

List of Figures

Research Disclaimer

This research brief is provided for informational and educational purposes and reflects analysis from SecureFi Institute on emerging computing technologies and cybersecurity trends. The views expressed are intended to support awareness and discussion of technology and infrastructure challenges and do not represent official policy positions.