

Memos to the PRESIDENT

Quantum Computing

Special Competitive Studies Project

SPECIAL COMPETITIVE STUDIES PROJECT



Subject:		Securing American Quantum Primacy
Purpose:		This memorandum presents a strategy to secure America's future as the world leader in quantum technologies, especially quantum computing.
Objectives:		Given quantum technology's dual-use capabilities, it remains imperative that the United States maintain its lead in research and development as these technologies become commercialized.
	1.	Achieve and Maintain Quantum Leadership
	2.	Accelerate Public-Private Coordination
	3.	Ensure Quantum Security and Resilience

Background

Quantum computing is poised to be a groundbreaking force in transforming civilization, so much so that some have called it the most important invention since fire.¹ It offers the potential to solve complex, compute-intensive problems beyond the reach of classical computers we use today. Imagine the power of quantum computer modeling integrated with the best available AGI systems on classical computers. That combination could revolutionize fields like medicine, accelerating drug discovery and enabling personalized treatments, as well as optimized investing and decision-making. The National Institute of Standards and Technology has even developed "post-quantum" encryption standards to survive the intelligence gathering power of large quantum machines.² As of 2024, the quantum computing market was projected to create 450-850 billion in economic value globally by 2040.³

Given the strategic importance of quantum technology to national power, the United States and China are engaged in a contest for quantum primacy. This competition is shaped by three major factors: China leads in quantum publications, but United States publishes significantly more high-impact, meaningful quantum computing research; the United States has a larger quantum ecosystem with 300 startups and 320 investors compared to China's 30 and 50; and China has invested approximately \$15 billion in

¹ Mark Whittaker, <u>We Don't Guess': Peter Barrett has 10 Unicorns Corralled in his Playground and He's Hunting More</u>, Forbes Australia (2024).

² Post Quantum Cryptography, National Institute of Standards and Technology (last accessed 2025).

³ Quantum Computing On Track to Create Up to \$850 Billion of Economic Value By 2040, Boston Consulting Group (2024).

quantum research, while the United States has invested \$4 billion.⁴ The first nation to master these technologies will gain unparalleled strategic advantages in secure communications, defense, AI, and data analysis that could reshape global power dynamics.

In addition to these competitive factors, strategic challenges remain in achieving a commercially viable quantum computer for all nations involved, including quantum error correction (QEC), decoherence, and quantum noise. Addressing these issues in quantum computing will also benefit advancements in quantum communications and sensors, creating a feedback loop that accelerates progress across all three technologies, ultimately driving commercial viability and strengthening national security. These challenges are:

- *Technological Gaps*: Much of current quantum technology, outside of quantum sensors, still requires breakthroughs to be commercially viable. The nation that deploys the first commercial quantum computer will have a first-mover advantage. Current hurdles include: limited scalable quantum hardware infrastructure, QEC and stability challenges, insufficient development of quantum algorithms, and constraints on talent and workforce development.
- *Competitive Investing Landscape Challenges*: The People's Republic of China (PRC) has heavily invested in quantum technologies \$13 billion compared to the United States' \$4 billion in cumulative public funding.⁵ Moreover, China has adopted a more controlled approach to knowledge sharing, withholding details of its own advancements, which gives it a strategic advantage in global quantum competition.
- *Fragmented U.S. Research Ecosystem:* While private industry contributes to quantum computing (QC) research, competing efforts in different quantum computing modalities (e.g., superconducting, photonic, atomic) are fracturing our national technological potential. This fragmentation hampers collaboration and progress within the Quantum Information Science (QIS) ecosystem.
- Long-Term Investment Barriers: Quantum computing startups face severe capital challenges. The extended development timeline deters private investment, creating a funding gap that threatens our national technological security. Without strategic financial support, many promising quantum computing initiatives risk stalling before reaching commercial maturity.
- Support Infrastructure Deficiencies: The rapid advancement of quantum computing necessitates the development of specialized support infrastructure, including advanced fabrication facilities and cryogenic systems. Quantum computers require extremely low temperatures and precise environmental controls to maintain qubit stability and coherence.⁶ Current semiconductor fabrication facilities are not equipped to meet these stringent requirements, and the lack of dedicated cryogenic infrastructure poses a significant barrier to scaling quantum technologies. Addressing these infrastructure gaps is crucial to ensure that U.S. companies can access vital components and effectively scale quantum systems.

⁴ Welcome to the Arena: Who's Ahead, Who's Behind, and Where We Are Headed Next in the U.S.-China Technology Competition, Special Competitive Studies Project (2025).

⁵ Alex Challans, CEO of Quantum Insider, speaking at the World Quantum Congress (2024).

⁶ Josh Schneider & Ian Smalley, What is Quantum Computing, IBM (2024).

Recommendations

Objective 1: Achieve and Maintain Quantum Leadership

The United States must prioritize achieving and sustaining leadership in all quantum information sciences (QIS) – quantum sensing, communications, and computing.⁷ By advancing research and development in quantum computing specifically and integrating it with developments in quantum communications and quantum sensors, the United States will secure a first-mover advantage in industries critical to national security, economic growth, and global competitiveness. Achieving quantum primacy⁸ will directly impact defense capabilities critical to the nation's security including secure communications, artificial intelligence (AI) applications, and high-performance computing.

• Elevate the National Quantum Initiative (NQI)

The NQI from the Office of Science and Technology Policy (OSTP) should be moved to a higherlevel coordination body, such as the Office of the Vice President (OVP), to make decision-making for the nation's quantum strategy more agile. Centralizing quantum initiatives under OVP will streamline decision-making, reduce redundant research efforts, and improve resource allocation efficiency. This reorganization optimizes federal quantum spending by enabling faster technology transfer between agencies and reducing administrative overhead.

NQI should foster collaboration by hosting a robust, monthly consortium of national quantum programs across a range of critical departments to accelerate breakout. This should include the QIS centers established under NQI, as well as the Department of Energy (DOE) Office of Science. The goal is to promote the exchange of existing quantum research at National Laboratories while facilitating collaboration on future R&D efforts for QIS.

Additionally, to strengthen strategic analysis within the NQI, the NQI's Subcommittee on the Economic and Security Implications of Quantum Science (ESIX) should expand its responsibilities to focus on technology strategy, forecasting, and competitive analysis across quantum technologies, with a primary emphasis on quantum computing.

• Increase Federal Funding for Quantum R&D

To support the Industries of the Future (IOTF) movement and maintain U.S. leadership in quantum technologies, The Federal Government should increase funding for quantum information science. This funding is essential to facilitating quantum computing breakout within the United States and ensuring the United States retains its competitive edge over global leaders, which has invested heavily in quantum research.

The National Quantum Initiative Act (NQI), representing \$1.3 billion of the U.S. Government's total \$4 billion investment in quantum technologies, has served as the cornerstone for advancing these technologies.⁹ As the leading program for coordinating and prioritizing the nation's quantum strategy, the NQI has been instrumental in fostering collaboration between federal agencies, academic

⁷ What is Quantum Information Science (QIS)?, National Institute of Health (last accessed 2025).

⁸ Barry C. Sanders, <u>Quantum Leap for Quantum Primacy</u>, Physics Magazine (2021).

⁹ Public Law No: 115-368, <u>National Quantum Initiative Act</u> (2018).

institutions, and private industry to build a robust quantum ecosystem. However, the rapidly intensifying global race for quantum primacy demands an accelerated investment strategy. Even with the United States' cumulative public funding of \$4 billion, current investment levels still trail behind global competitors.¹⁰ The Chinese government, for example, has invested an estimated \$13–15 billion towards developing quantum technologies, highlighting the need for an increase in federal funding.¹¹

In addition to the increased funding, the U.S. Government should establish more consistent and targeted quantum technology grant programs in tandem with grand challenge prizes. These programs, modeled on previous, successful National Science Foundation (NSF) and DOE awards that resulted from NQI's implementation, should support both academic institutions and private industry in building the entire quantum ecosystem. These grants and challenges should focus on addressing specific technical challenges in quantum computing, providing sustained long-term funding mechanisms to support both incremental advancements and breakthrough innovations, with the ultimate goal of achieving commercially viable quantum technologies.

Specifically, the Federal Government should consider \$1 billion from FY 2026 to FY 2029 annually for quantum communications and quantum sensing efforts. Additional funding of \$2 billion annually should be allocated to research and development efforts in the top three most promising quantum computing modalities. In addition, infrastructure funding should be provided to ensure access to critical components and enable large-scale experiments, accelerating the development and testing of quantum technologies ahead of global competitors.

This investment strategy balances fiscal prudence with the imperative to secure U.S. quantum leadership. It accelerates the commercialization of quantum computing, communications, and sensing while remaining competitive with the scale of investment currently seen from international adversaries. By investing swiftly and decisively, the United States can retain its leadership position in this transformative field.

Objective 2: Accelerate Public-Private Coordination

To catalyze breakthroughs in quantum technology, the United States must increase federal investment in quantum research and development. This includes both direct funding to quantum initiatives and supporting a more cohesive and strategic national quantum ecosystem. Federal agencies, universities, and the private sector must align their efforts to ensure that quantum technology is developed at scale, remains secure from foreign adversaries, and is positioned for rapid commercialization. Centralized leadership within the federal government will foster an agile and responsive approach to quantum development efforts.

• Launch a National Quantum Excellence Program (NQEP)

This program would serve as a strategic coordination body to unify cross-organizational learning from quantum computing efforts across the national ecosystem, bringing together private entities, federal agencies like DARPA, and research institutes. By leveraging existing quantum initiatives, in particular, efforts like the Quantum Economic Development Consortium (QED-C) and the Quantum Benchmarking Initiative, the NQEP would create a unified approach to developing commercially viable quantum technologies, facilitate knowledge-sharing, and reduce redundancy. Housed under the National Quantum Initiative and reporting directly to its program manager, NQEP would

¹⁰ Alex Challans, CEO of Quantum Insider, speaking at the World Quantum Congress (2024).

¹¹ Alex Challans, CEO of Quantum Insider, speaking at the World Quantum Congress (2024).

facilitate knowledge exchange between DARPA's quantum initiatives, QIS centers, and the DOE Office of Science, creating a streamlined pathway for quantum computing research and development.

• Establish a National Quantum Moonshot

The United States should develop a one million qubit fault-tolerant computer with interconnect output to classical computers by 2028.¹² This is seen as a crucial milestone to move beyond theoretical demonstrations and lab experiments to tackle industrial-scale, real-world problems that are currently intractable for even the most powerful classical computers.¹³ Many problems, like designing new materials, producing tailored medicines, optimizing complex logistics, or modeling systems like the stock market require simulating very large and intricate systems that are thought to require at least one-million-qubit sized quantum computers. Simulations for examples like these demand a massive number of qubits to represent the complexity accurately.

Objective 3: Ensure Quantum Security and Resilience

Quantum technology holds immense promise but also presents national security risks. The United States must take proactive measures to prepare for the post-quantum world and the impact of quantum computing on cybersecurity and defense systems. Quantum computers have the potential to break widely used encryption algorithms, such as RSA and ECC.¹⁴ These algorithms are critical to securing communications, financial transactions, and other vital systems across sectors like banking, government, and healthcare. If compromised, they could undermine the security of current encryption standards. Additionally, the United States must ensure the resilience of its quantum ecosystem by protecting its infrastructure from both natural and adversarial threats, creating a secure and reliable quantum technology supply chain insulated from adversarial risks.

• Form an Offensive Capabilities Unit within the NQI

As quantum technologies progress and become commercially viable, standards must be upheld across the United States to prevent strategic surprise from our adversaries. A dedicated unit focused on quantum-related offensive capabilities, including disruption strategies, counterintelligence efforts, and monitoring global quantum advancements and supply chains, would allow for a proactive, continuous assessment of both quantum threats and vulnerabilities, as well as opportunities for strategic advantage. This unit would perform threat analysis to pinpoint areas where adversarial states might disrupt supply chains or gain access to sensitive information, while also conducting opportunity analysis to uncover areas where strategic investments could drive leadership and technological advancements. This unit could be housed within the ESIX under NQI, as a standalone unit within NQI, or at a relevant government agency.

This unit should also collaborate with agencies like the National Institute of Standards and Technology and the Department of Defense to develop preventive measures against adversarial uses of quantum technologies, with a particular focus on post-quantum cryptography and quantum computing.

¹² <u>National Action Plan for U.S. Leadership in Advanced Compute & Microelectronics</u>, Special Competitive Studies Project (2023).

¹³ See e.g., Chetan Nyak, <u>Microsoft Unveils Majorana 1, The World's First Quantum Processor Powered by Topological Qubits</u> (2025).

¹⁴ RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC) are both public-key cryptographic algorithms that use different mathematical functions to encrypt and decrypt data. RSA relies on factoring large numbers, while ECC uses complex curves—ECC is considered more efficient and harder to break with quantum computers. Both are used to secure data and communications in critical sectors such as the financial, healthcare, and defense sectors.

Conclusion

This strategy is not just about technological development—it's about maintaining America's global technological dominance. By acting decisively, investing strategically, and unifying our quantum research ecosystem, the United States can establish absolute quantum primacy.