ORION FORUM

Post-Quantum Cryptography: An Urgent Need for AI Infrastructure

JANUARY 17, 2026

Post-quantum cryptography is typically framed as a problem in quantum computing. It is something to address once fault-tolerant machines arrive. So, this framing is still incomplete. Every scaled AI system today depends on encrypted data pipelines, protected model weights, and secure inference infrastructure. The cryptographic standards protecting that infrastructure are already quantum-vulnerable. This means the growth story of artificial intelligence is inseparable from the security transition now underway. Therefore, the real competitive separation between companies and nation-states is shifting from who has AI to who can industrialize intelligence through governed, secure, and compounding systems across products, supply chains, and critical infrastructure.

That is where quantum intelligence enters the frame, not only as a distant science project, but as a near-term forcing function that American firms and policymakers can no longer defer. In reality, “quantum readiness” doesn’t mean waiting for a completely fault-tolerant device. It focuses on strengthening the foundations that AI relies on: security, cryptography, and resilience, while developing the hybrid computing pathways that will define the next era of high-value workloads.

The merging of these technologies is already happening.

Two developments collapsed the timeline between “AI strategy” and “quantum readiness.”

First, the National Institute of Standards and Technology (NIST) finalized the first post-quantum cryptography standards in August 2024. Building these standards wasn’t actually a research milestone, but it was just the starting point. Therefore, any organization with sensitive data, such as healthcare systems, financial institutions, defense contractors, and critical infrastructure operators, now initiates a migration program measured in years rather than

decades.

Cybersecurity and Infrastructure Security Agency (CISA) has become explicit about what comes next, such that it builds a cryptographic inventory, engages vendors, and starts planning and testing transitions now, not later. CISA does not postpone its policies anymore. It comes, therefore, with the operational reality of “quantum readiness”, a concrete, multi-year engineering program, not a speculative bet.

Second, quantum hardware progress is becoming more legible to non-specialists because the field is increasingly measured in “error-correction reality,” not qubit counts. In late 2024, Google reported a quantum error-correction milestone with its Willow processor, demonstrating that error-corrected performance improves as systems scale, a significant signal for anyone tracking the path to reliable quantum machines.

Meanwhile, IBM’s roadmap is also more explicit about hybrid quantum-classical operation, using classical high-performance computing (HPC) to extend what can be run and mitigated in near-term systems. The direction is clear now, such that the commercial “shape” of early quantum value will become hybrid, not purely quantum like physics.

Nevertheless, the strategic implication is straightforward. AI and quantum are not bets that will eventually be sequential. They are becoming operationally entangled. Having said that, AI systems generate large data volumes, security requirements, and optimization bottlenecks that push compute strategy to its limits. Post-quantum cryptography is therefore not a ‘quantum problem’ but an AI deployment prerequisite, such that organizations building AI infrastructure without crypto-agility are accumulating technical debt that will force costly retrofits. So, treating them as separate line items may turn into a planning failure.

What this means for American competitiveness

As expected, China treats AI and quantum together as adjacent strategic priorities and acts accordingly. Its 14th Five-Year Plan explicitly links quantum computing and AI as named as “frontier technologies” requiring coordinated state investment, with dedicated national laboratories and integration into industrial policy. Clearly, China is not rhetorically positioning itself in this dynamic domain, but it actually keeps allocating essential resources.

On the other hand, Europe is interestingly moving faster on governance. The EU AI Act was issued on August 1, 2024, with staggered obligations, including bans on certain practices. Further, AI literacy requirements began in February 2025. Even general-purpose AI obligations became active in August 2025 and will be fully enforced in August 2026.

Meanwhile, the United States still holds real advantages with its world-class research institutions, deep capital markets, and hyperscale's commercializing both AI and quantum. However, these advantages do not make the USA a leader in this domain without coherent coordination across the states. Nevertheless, American companies are increasingly navigating a fragmented landscape of state-level AI governance regulations. In fact, over 40 states introduced AI-related bills in 2024 alone, creating domestic compliance friction and global market uncertainty.

AI adaptation is not enough for the USA in this competitive world. It needs to treat AI-quantum convergence as a competitiveness agenda spanning cybersecurity, R&D integration, procurement, and governance, aiming for a robust computing advantage with quantum intelligence.

Three policy moves that would strengthen America's hand

1. **Treat post-quantum migration as critical-infrastructure policy, not just cybersecurity hygiene.**

The NIST standards are finalized. The technical direction also seems clear enough. What's missing now is urgency and consistent execution. In fact, federal agencies and critical infrastructure sectors should be driven toward measurable milestones, including cryptographic inventories, vendor-readiness assessments, and staged migrations for high-value systems and long-lived data. To ensure coherent federal action, the Department of Homeland Security and the Department of Commerce should jointly oversee transition timelines. CISA's guidance provides the operational steps. Then, policy should translate them into procurement incentives that reward an early quantum-safe posture.

2. **Accelerate hybrid compute R&D through existing National Quantum Initiative channels.**

As AI and quantum technology converge, the most practical near-term quantum applications will not be standalone quantum programs. They will be hybrid workflows, quantum devices handling narrow subroutines within classical AI and HPC pipelines, with software, tooling, and error mitigation doing the heavy lifting. The National Quantum Initiative framework exists precisely to coordinate federal effort; the priority now should be integration of research and deployment pathways, not hardware milestones alone. Funding criteria should reward demonstrated hybrid workflows, such as quantum subroutines integrated into classical AI pipelines, rather than just qubit counts.

3. **Align AI governance with quantum-era security requirements without importing a rigid regime.**

The United States does not have to follow Europe's model to build a strong strategy. However, without a clear federal standard, liability remains uncertain, and U.S. companies face more challenges in global operations. A simple framework that focuses on transparency, auditability, security by design, and crypto-agility, including clear plans for post-quantum migration in sensitive systems, can boost competitiveness and support ongoing innovation. The other option is to let things drift, which means companies would have to deal with different rules in each state and face tougher requirements in other countries.

For American companies, having a federal governance baseline is not only about making rules clearer at home. It also helps level the playing field by reducing the compliance gap that now gives European competitors an edge in global procurement.

The real depiction of "pioneer."

People still call any company with the most impressive demo an "AI pioneer." But that idea is outdated. By 2026, a true pioneer will be an organization or country that can build intelligence into its systems from the ground up. This means being secure against future (post) quantum threats, following clear rules, and ensuring new abilities build on each other rather than spreading out without focus. Europe is creating a strong position with clear regulations. China is treating AI and quantum computing as key priorities and investing in both. The United States still leads in turning ideas into products, but it could lose its edge if it continues to plan in separate silos and lacks unified direction.

Bringing these technologies together does have risks. If AI and quantum systems are combined too soon, and their connections are not properly checked, new security problems could appear. The European Union has introduced a voluntary code of practice to help businesses comply with the new AI Act, aiming to encourage responsible progress in artificial intelligence. While overly restrictive regulations could slow down intended advancements, supporting compliance may be preferable to the risks of inaction. If the U.S. does not act, other countries may be able to set the rules and dominate markets for critical technologies like post-quantum cryptography, potentially putting national security and technological leadership at risk.

A joint statement from CISA, NIST, and the NSA emphasizes that American companies and policymakers have the knowledge and resources essential to lead in this area. The real question is whether they will approach AI and quantum as a single strategic system, combining security, computing, and governance, or keep handling them separately until a competitor or adversary demonstrates what true integration means.

The window for shaping that answer is open. But it will not stay open long. NIST has signaled that quantum-vulnerable algorithms will be deprecated by 2030 and removed from standards by 2035; organizations that delay will face compressed timelines and higher costs.
