Rethinking the “Impossible”: Why Quantum Computing Demands Urgent Post-Quantum Preparation

[Excerpt – Introduction to Full Report]

For decades, quantum computing has existed in a liminal space between scientific aspiration and theoretical impossibility. The gap between today’s binary architectures and the probabilistic, superposition-driven quantum paradigm is so vast that the commercial world still treats quantum viability as a problem for 2050 or beyond. This mindset, while understandable, misses the deeper strategic reality: we do not need commercial-grade quantum devices for quantum-level risk to arrive. We only need one nation-state, one intelligence service, or one deeply resourced organization to develop a quantum-like capability capable of breaking today’s cryptographic assumptions.

This asymmetry (where the threat emerges long before the benefits) creates a policy and security landscape far more urgent than public discourse suggests. While companies debate potential efficiencies and longer-term computational breakthroughs, the cryptographic foundations of global finance, medical records, private communication, and national security infrastructure are already nearing obsolescence. Algorithms like RSA and ECC, which underpin most secure digital exchanges, are vulnerable the moment a quantum adversary appears, even if such an adversary is years ahead of commercial timelines.

This report begins by reframing quantum computing not as an engineering milestone but as a geopolitical accelerant. It explores why “harvest now, decrypt later” strategies are already in play, how quantum-adjacent computation (including annealers and hybrid systems) accelerates the threat timeline, and why post-quantum cryptographic standards must be adopted far earlier than organizations expect.

The central argument is simple: quantum risk is not a future scenario because it is a present trajectory.

Our global posture must shift accordingly.