ISSUE 5

THIS WEEK IN QUANTUM SECURITY

June 23, 2026

By
Joel Van Dyk
Quantum Security Advisor and Strategist

One thing stood out this week.

The conversation around post-quantum cryptography is no longer just about future risk. It is becoming a question of certification, procurement, investment, regulation, and operational readiness.

For years, the debate focused on when quantum computers might become powerful enough to threaten today's public-key encryption. This week, the more important question was: how do governments, financial institutions, cloud providers, technology vendors, and critical infrastructure operators begin preparing before the transition becomes urgent?

That shift matters. As Phil Intallura put it, the word is "now."

THREE TRENDS WORTH WATCHING

1 The UK Moves From Strategy to Procurement

Patrick Vallance announced the UK Quantum Growth Alliance at London Tech Week. With major firms across finance, telecoms, energy, aerospace and defence, plus GBP1.2bn in procurement commitments, the signal is clear...

2 Certification, Investment and Markets Accelerate

France's ANSSI is moving quantum-safe encryption into certification from 2027. Reuters also reported a $500M U.S. award to SandboxAQ and EigenQ's planned $3B SPAC deal.

3 AI, Policy and Global Readiness Are Converging

AI-assisted work is optimizing quantum attack research, a new U.S. executive order sharpens federal direction, and Singapore, Japan, South Korea and China remain important markets to watch.

WHAT I'M READING

- **Phil Intallura: UK Quantum Growth Alliance**
  linkedin.com/in/intallura
- **Reuters: France quantum-safe certification**
  reuters.com/legal/litigation/france-stop-certifying-pro...
- **Reuters: SandboxAQ $500M materials award**
  reuters.com/technology/us-awards-500-million-nvidia-bac...
- **Reuters: EigenQ $3B SPAC deal**
  reuters.com/legal/litigation/quantum-tech-firm-eigenq-g...
- **NIST Post-Quantum Cryptography Standards**
  csrc.nist.gov/projects/post-quantum-cryptography
- **UK NCSC PQC Migration Guidance**
  ncsc.gov.uk/guidance/pqc-migration-timelines
- **Cloudflare Post-Quantum Roadmap**
  blog.cloudflare.com/post-quantum-roadmap/
- **White House: EO 14409 Advanced Cryptographic Attacks**
  whitehouse.gov/presidential-actions/2026/06/securing-th...
- **ECDSA.fail challenge**
  ecdsa.fail/
- **Singapore: Quantum Fortitude 2026**
  ddas.sg/quantum-fortitude
- **Toward Quantum-Safe 6G**
  arxiv.org/abs/2605.06881

ONE NUMBER TO WATCH

2027

France will stop certifying security products that do not include quantum-safe encryption. A clear signal that PQC is moving from advice to requirements.

CLOSING THOUGHT

Cryptographic agility is the theme that keeps coming up. The challenge is not choosing algorithms. It is building systems, partnerships, and processes that can adapt as standards, policy and threats evolve. The transition is a long-term journey, but preparation is already global.