ISSUE 7

THIS WEEK IN QUANTUM CRYPTOGRAPHY

July 3, 2026

By
Joel Van Dyk
Quantum Security Advisor and Strategist

Markets are closed in New York today as the United States prepares to mark the 250th anniversary of the Declaration of Independence.

That feels like the right moment to think about infrastructure.

Not roads, bridges, or ports this time, but the digital infrastructure that now underpins financial markets, government systems, identity, payments, communications, and trust itself.

In some ways, the post-quantum transition feels similar to the work many of us saw around the year 2000.

The risk was technical, but the response had to be operational.

Systems had to be found.

Dependencies had to be understood.

Vendors had to be coordinated.

Deadlines mattered.

Leadership mattered.

And while the world did not end at midnight, that was partly because a great deal of serious work happened before the deadline arrived.

Post-quantum cryptography has a similar feel.

It is scary, because the systems involved are vast, old, interconnected, and often poorly documented.

It is also exciting, because this is exactly the kind of problem cybersecurity was built to solve: technical risk translated into practical resilience.

This week, the signals continued to come from several directions at once. The United States is moving through executive authority. Europe is building a coordinated transition roadmap. France is using certification. Singapore is using readiness frameworks. The UAE is building national crypto-discovery capability.

Different tools.

Same direction.

Post-quantum cryptography is becoming part of how countries think about digital trust, critical infrastructure, procurement, and resilience.

The question is no longer whether post-quantum migration will happen.

The question is who will be ready first.

What's Been Happening

Because this week's theme is infrastructure, it is worth stepping back from the headlines and looking at how the landscape has evolved over the past month.

1 The U.S. Has Made the Timeline More Explicit

The U.S. issued a new executive order focused on advanced cryptographic attacks and post-quantum migration. The order recognises the risk of "harvest now, decrypt later" attacks and directs federal systems toward NIST-approved post-quantum cryptography standards.

What matters here is not simply the policy language. It is the market signal.

Once federal agencies and contractors are expected to transition, vendors, cloud providers, software companies, and critical infrastructure operators such as banks have to respond.

This is how guidance becomes procurement pressure.

2 Europe Is Building the Framework Before the Crisis

Europe is not waiting for a single dramatic quantum breakthrough.

The European Commission and the NIS Cooperation Group have set out a coordinated implementation roadmap for the transition to post-quantum cryptography. Member States are expected to begin transition activity by the end of 2026, with critical infrastructure moving as soon as possible and no later than 2030.

This sits naturally alongside NIS2, DORA, critical infrastructure protection, financial-sector resilience, and digital sovereignty.

In other words, Europe is treating post-quantum cryptography as part of the broader resilience stack.

What is interesting is that Europe is not waiting for a single regulatory event. It is building a framework where policy, resilience, procurement, and operational security reinforce one another. That may ultimately prove to be one of Europe's biggest competitive advantages.

3 France Is Moving Through Certification

France may be one of the clearest national signals right now.

ANSSI has indicated that, beginning in 2027, it will stop certifying security products that do not include quantum-safe encryption.

That matters because certification changes buying behaviour.

Vendors selling into sensitive environments will need to demonstrate quantum-safe capability, not simply say they are watching the space.

France is effectively saying: if you want trust, you need a migration path.

4 Singapore Is Taking a Practical Approach

Singapore is worth watching closely.

The Cyber Security Agency of Singapore has published a Quantum-Safe Handbook and Quantum Readiness Index to help organisations assess readiness and begin the transition. Singapore is treating post-quantum cryptography as the mainstream path for broad quantum-safe migration, while recognising that quantum key distribution may have more specialised use cases.

That is a useful distinction.

Singapore is not making the conversation unnecessarily complicated. It is asking organisations to understand risk, assess exposure, build capability, and prepare in a structured way.

For a global financial and cybersecurity hub, that matters.

5 The UAE Is Moving Into Crypto Discovery

The UAE is also becoming an important signal.

The UAE Cyber Security Council has partnered with QuantumGate to launch a national Crypto Discovery Tool as part of its post-quantum migration programme.

This is important because discovery is the hard first step.

You cannot migrate cryptography you cannot see.

The UAE's approach is notable because it is focused on visibility, inventory, continuous monitoring, and readiness across sectors. That moves the conversation from policy into operating capability.

Discovery is not glamorous, but it is foundational. Before organisations can replace cryptography, they first have to know where it exists. In many ways, the UAE is solving the first problem before trying to solve the second.

6

Cloud, Telecoms, and the Internet Layer Are Showing the Deployment Gap

The research side is also becoming more practical.

A recent measurement study of more than 32,000 domains found partial progress toward post-quantum readiness, but also major gaps. Hybrid post-quantum key exchange is appearing in some places, but certificate infrastructure and authentication remain far less mature.

This is the key point.

Post-quantum migration is not only about protecting key exchange.

It also has to include certificates, identity, authentication, vendor dependencies, and operational tooling.

That is where the real work begins.

What I'm Watching in July

Events and Conferences

• GITEX Quantum Expo Europe - Berlin, 30 June-1 July 2026

Quantum is being positioned alongside AI, advanced semiconductors, space, biotech, and dual-use technology. That tells us something important: quantum is increasingly viewed as strategic infrastructure, not only academic research.

https://www.gitexeurope.com/Quantum-Expo

• Quantum.Tech Europe - Delft, Netherlands, 13 July 2026

A useful event to watch because the focus is on practical applications across finance, healthcare, logistics, and cybersecurity. This is where the conversation moves from research into implementation.

https://qutech.nl/event/delftquantumshowcase-copy/

• IEEE ISIT 2026 - Guangzhou, 28 June-3 July 2026

Not a post-quantum migration conference specifically, but relevant for the theoretical foundations around information, communication, coding, and security.

https://www.squad-germany.de/en/events-2/

• Looking Ahead: TQC 2026 - Sherbrooke, Canada, 31 August-4 September 2026

The Theory of Quantum Computation, Communication and Cryptography conference remains one of the key academic meetings for theoretical quantum information science.

https://quantumcomputingreport.com/conferences/

• Looking Ahead: PQC + IQT - New York, 25-26 October 2026

Worth tracking for the intersection of post-quantum cryptography, industry deployment, and quantum technology.

https://iqtevent.com/

• Looking Ahead: Q2B26 x Chicago Quantum Summit - Chicago, 8-10 December 2026

This event will bring together industry, government, and academic leaders from around the world for dialogue aimed at shaping the future of quantum technology. Hosted by QC Ware and the Chicago Quantum Exchange.

https://q2b.qb3.org/chicago-quantum-summit

Papers and Research Worth Reading

• Measurement Study of Post-Quantum Readiness of Internet: 2026

This paper is useful because it moves the discussion from opinion into measurement. It examines real-world TLS deployments across more than 32,000 domains and highlights the uneven state of post-quantum readiness.

https://arxiv.org/abs/2606.16473

• quantum-safe: Bridging the Post-Quantum Production Gap with a Hybrid-by-Default Python Cryptography Library

This paper focuses on the practical gap between standards and production deployment. That gap is where many organisations will struggle.

https://arxiv.org/abs/2605.17061

• Toward Quantum-Safe 6G: Experimental Evaluation of Post-Quantum Cryptography Techniques

Important because 6G, edge devices, bandwidth constraints, and latency all expose the practical trade-offs of post-quantum deployment.

https://arxiv.org/abs/2605.06881

• Shaping a Quantum-Resistant Future: Strategies for Post-Quantum PKI

PKI is one of the most important and difficult parts of the transition. This paper is useful for understanding certificate infrastructure, revocation, and the operational challenge of moving authentication into a quantum-resistant model.

https://arxiv.org/abs/2601.11104

Why It Matters

The phrase that keeps coming up is still cryptographic agility.

Not just stronger encryption.

Adaptable infrastructure.

The organisations that manage this transition well will be the ones that can identify where cryptography exists, understand dependencies, coordinate vendors, update procurement requirements, test hybrid deployments, and prove progress to regulators and boards.

That is a different kind of security problem.

It is not solved by one algorithm.

It is solved by governance, architecture, inventory, testing, and the ability to adapt as the standards and threat models evolve.

The quantum threat remains a long-term challenge.

The preparation phase is already here.

History rarely remembers the organisations that waited until the deadline.

It remembers the ones that recognised the transition early enough to build resilience before everyone else realised it was necessary.

ONE NUMBER TO WATCH

32,000+

A recent measurement study examined more than 32,000 domains and found that post-quantum readiness is uneven. Key exchange is starting to move, but certificates, authentication, and operational tooling remain far less mature.

This Week in Quantum Cryptography is a weekly briefing on the global transition to post-quantum security. It follows the policies, research, technology, and market developments shaping the future of cryptography, with a particular focus on financial infrastructure, critical systems, and enterprise cyber resilience.

- Joel Van Dyk