POST-QUANTUM READINESS / THE 250TH YEAR

Washington's Secrets Survived the British. Yours May Not Survive the Decade.

A 250th-birthday reading of the quantum threat. The traffic being harvested today does not need a quantum computer yet. It only needs you to keep waiting.

QTONIC QUANTUM RESEARCH TEAM | JULY 6, 2026

The United States turned 250 this weekend. The speeches covered muskets and parchment and mostly skipped the part where the war was run on encrypted mail. George Washington operated one of the more disciplined intelligence networks of his century, and its tradecraft reads as strikingly modern. Code books in which the number 711 meant Washington himself. Cover names for agents who never signed anything. Invisible ink brewed by a physician and rationed like ammunition. The founders did not treat secure communication as a technicality. They treated it as the difference between a republic and a list of hanged men.

Two hundred fifty years later the republic still runs on secrets, and the mathematics protecting them now has a named successor. The reason to act is not a date on anyone's roadmap. Harvest-now attacks make long-lived data exposed today, a cryptographic migration runs for years, and the gating first step, a cryptographic inventory, is the one most organizations have never run.

There is a quieter anniversary inside the loud one. Public-key cryptography, the mathematics that authenticated nearly everything you did on a screen this morning, was published in 1976, the year of the bicentennial. The trust layer underneath American commerce turns 50 as the country turns 250. Only one of the two is aging well.

The first American network

Start with what the founders actually built. In 1778, Washington's intelligence chief Benjamin Tallmadge organized the Culper Ring to report from British-held New York. Its operators used a code book of more than 700 numbered entries, cover identities they kept for years, dead

drops, and a sympathetic stain developed by James Jay that turned a blank page into a report when brushed with a second chemical. The ink was scarce enough that Washington personally managed who received it. None of these measures was unbreakable on its own. What kept the network alive was that its operators could enumerate it. Tallmadge knew which copies of the code book existed, which routes carried traffic, and which hands held the ink.

The most famous cryptographic failure of the era came from inside. Benedict Arnold negotiated his treason with the British in ciphered correspondence, and the plot collapsed not because the cipher broke but because a courier was searched and the plans of West Point came out of John André's boot. The lesson outlived him. Cryptography fails at the places nobody is watching, and the fatal gap is rarely the mathematics.

The mathematics of the bicentennial

The second anniversary is the one your infrastructure cares about. In November 1976, Whitfield Diffie and Martin Hellman published "New Directions in Cryptography" and solved a problem Washington would have paid a brigade for. Two parties who have never met can establish a shared secret over a channel the enemy is reading. RSA followed within a year. Nearly everything since is built on that foundation. The certificate that vouches for your bank, the handshake underneath every secure connection, the signature on every software update, the keys that hold VPNs and identity systems together. All of it rests on a small family of mathematical problems that are hard for the computers we have.

In 1994, Peter Shor showed those problems are not hard for a sufficiently capable quantum computer. No machine able to run his algorithm at that scale exists in public today. But the endgame is settled enough that in August 2024 NIST finalized the replacement standards, FIPS 203, 204, and 205. That was the state of things on the republic's 250th birthday, and the weekend did not change it. The successor is named, the predecessor is everywhere, and most organizations cannot say where.

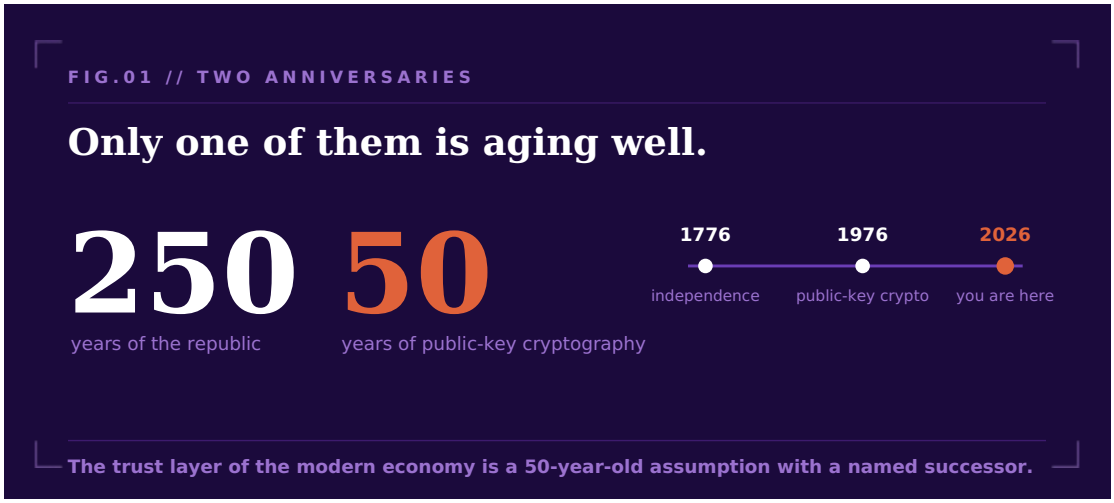


FIGURE 1 · TWO ANNIVERSARIES. Public-key cryptography dates to the Diffie-Hellman publication of November 1976. The pairing of anniversaries is an editorial observation. Sources at the foot of this article.

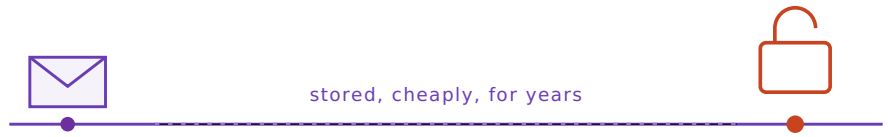
The intercept does not expire

Here is where the birthday framing stops being sentimental. In 1780, an intercepted dispatch had a shelf life. Once the troops moved, the secret died on its own, which is why a captured courier was a crisis measured in weeks. The modern intercept is patient, and it does not observe federal holidays. Whatever traffic was being recorded before the holiday was still being recorded while the fireworks went up. An adversary who records encrypted traffic today can store it for pennies and decrypt it whenever a capable machine arrives. The technique has a name, harvest now, decrypt later, and it inverts the old arithmetic. The question is no longer when quantum computers arrive. The question is how much of what you transmitted this year still needs to be secret on that day.

Run the numbers the way Michele Mosca's widely cited framing suggests. Add the years your data must stay confidential to the years a full migration takes. If the sum is larger than the years until a capable machine, you are already late, and for health records, deal terms, government archives, and core intellectual property, the sum is larger for most realistic estimates. That is why the exposure is present tense. It began at capture, not at decryption.

FIG.02 // THE PATIENT INTERCEPT

Exposure begins at capture, not at decryption.



captured 2026
still encrypted

readable at machine arrival
date unknown, outcome not

For long-lived data the clock started at capture. Waiting shortens nothing except your options.

FIGURE 2 · THE PATIENT INTERCEPT. The timeline is illustrative. Whether any given traffic has been captured is unknowable by design, which is the point of treating long-lived data as exposed. Sources at the foot of this article.

The signature does not forgive

Harvest-now attacks explain why confidentiality is already exposed. Authentication explains why the blast radius is wider. A cryptographically relevant quantum computer would not only read what was once secret. It could forge the signatures and trust chains that decide who is allowed to sign code, issue a certificate, authenticate a device, approve an update, and prove identity. Confidentiality is a question about the past, the traffic already captured. Authentication is a question about the future, every system that will trust a credential tomorrow.

That is why the serious roadmaps separate key establishment from signatures, and why the platform vendors say the signature migration is the harder of the two. Encryption protects what was said. Authentication decides who gets believed. Microsoft lists certificate issuance, code signing, key protection, and update pipelines among the most complex areas of its own transition, which is a plain admission that the second problem outlasts the first.

The month the signals converged

The 250th birthday also lands at the close of a month that will read, in hindsight, like a hinge. The signal did not arrive as one announcement. It arrived as four layers moving at once.

The timeline compressed in four places

The science layer changed first. Google Quantum AI published an updated resource estimate for attacking the elliptic-curve problem that sits under much of today's public-key cryptography, needing fewer logical qubits and gates than earlier planning models assumed. A separate theoretical architecture from a Caltech-led group suggested Shor's algorithm could reach cryptographic scale with far fewer physical qubits than older estimates required. Neither paper proves a capable machine arrives in 2029. Both move the downside of waiting,

which is the one variable a defender actually controls.

Then the platform layer moved. Google set a 2029 post-quantum migration timeline. Cloudflare moved its full post-quantum protection target to 2029. Microsoft followed with a 2029 target for its critical products and services, and made the operational point plainly. The hard part for most organizations is not choosing algorithms. It is understanding and updating where cryptography already exists across applications, services, networks, identities, certificates, and hardware.

Then the policy layer moved. France said it would stop certifying security products that lack quantum-resistant encryption from 2027. That is not guidance. It turns quantum resistance into product eligibility, because from 2027 a product without it risks losing certification for French government and critical-infrastructure use, which is how a security standard becomes a procurement standard. Days earlier the United States ordered accelerated federal migration to NIST-approved post-quantum cryptography and reached contractors through the acquisition rules.

Then OMB made the board-level point explicit. Its memorandum implementing the executive order, M-26-15, directs agencies to produce dynamic cryptographic inventories, a cryptographic bill of materials, prioritized migration plans with named owners and funding, supplier coordination, and continuous monitoring, on a clock that starts this year. That is no longer a research signal. It is operating doctrine, and it names the exact evidence a buyer will soon expect to see.

Read together, the four layers say one thing. 2026 is the year post-quantum readiness moved from a future risk to an evidence requirement.

FIG.03 // THE 2026 COMPRESSION STACK

Four layers, one direction.

LAYER	WHAT CHANGED	BOARD MEANING
SCIENCE	Resource estimates moved down	Risk window narrowed
PLATFORMS	Google, Cloudflare, Microsoft to 2029	Vendors stopped waiting
REGULATORS	France 2027, US order 2026	PQC becomes eligibility
OMB M-26-15	Inventory, CBOM, owners, budget	A funded control now
ENTERPRISE	Customers ask for evidence	**"We monitor it" fails**

The question is no longer whether PQC is real. It is whether you can prove where it is exposed.

FIGURE 3 · THE 2026 COMPRESSION STACK. Layer descriptions summarize documented 2026 announcements and guidance. The reading that they form a single compression event is Qtonic Quantum analysis. Sources at the foot of this article.

DOCUMENTED FACT. NIST finalized FIPS 203, 204, and 205 in August 2024. The French certification guidance was reported June 16, 2026. The US executive order was signed June 22, 2026. Microsoft announced its accelerated 2029 goal on June 30, 2026, identifying inventory and discovery as the primary challenge. OMB memorandum M-26-15 directs federal agencies to execute the migration through cryptographic inventories, a cryptographic bill of materials, migration plans with owners and funding, and continuous monitoring. Google Quantum AI published a lowered resource estimate for attacking elliptic-curve cryptography, and a Caltech-led group published a theoretical architecture toward the same end. Both are estimates and theory, not demonstrated breaks. Public-key cryptography was published by Diffie and Hellman in November 1976, and Washington's Revolutionary War networks used ciphers, numbered codes, cover names, and invisible ink.

REASONABLE INFERENCE. When standards bodies, regulators, and the platform layer converge on the same first move within a short window, the practical timeline for everyone downstream compresses, whatever any single deadline says. This is analysis, not a statement by any of the parties named.

STRUCTURAL RISK ANALYSIS. Because harvest-now-decrypt-later means long-lived data captured today can be exposed once a capable machine exists, the exposure is present tense regardless of the arrival date. This is analysis, not a prediction of when any system breaks.

What the founders knew about inventories

Look again at why the Culper Ring worked, because the reason is not romantic. The network was small enough, and run tightly enough, that its operators always knew its full extent. Nothing carried traffic that Tallmadge had not placed there. Now invert every property of that picture and you have a modern enterprise estate, where cryptography has accreted for thirty years across applications, services, networks, identities, certificates, and hardware, much of it undocumented and some of it older than the staff maintaining it. Washington's operation would have called that state of affairs a network already penetrated. You cannot migrate the cryptography you have never found.

FIG.04 // THE TRADECRAFT MIRROR

The network survived because it could be mapped.

1778	2026
code book, numbered entries	algorithm and key inventory
cover names, held for years	identities and certificates
invisible ink, rationed	key custody and rotation
courier routes, memorized	protocols and endpoints
enumerated by its operators	**undocumented in most estates**

Discovery is the tradecraft. It always was.

FIGURE 4 · THE TRADECRAFT MIRROR. The pairing is illustrative, drawn from documented Culper Ring practices set against the standard elements of a modern cryptographic estate. Sources at the foot of this article.

What this means for a board

For a board, the second half of 2026 is no longer about whether quantum risk belongs on the register. The question is whether management can produce the evidence now being normalized by government and platform buyers: a dynamic cryptographic inventory, a cryptographic bill of materials, a prioritized migration plan with named owners, a funding estimate, third-party coordination, and a crypto-agility architecture. The first question has changed with it. The board no longer asks only when quantum will arrive. It asks whether you can prove what you must migrate, and the birthday is simply the year that made the question hard to miss.

Monday also opens the second half of 2026, and the half-year ahead already has dates on it. Federal agencies face an OMB migration-planning deadline in late October under the memorandum implementing the June executive order. The French certification cutoff arrives with the new year. Microsoft's 2029 target and the executive order's 2030 and 2031 milestones for key establishment and digital signatures are near enough that a multi-year program funded in this cycle is the kind that reaches them comfortably. The back half of the year is when the customer questionnaires start assuming you have begun.

What Qtonic Quantum brings to the 250th year

Qtonic Quantum starts where the new guidance starts, at discovery. QScout produces the live cryptographic map: exposed RSA and elliptic-curve dependencies, certificates, protocols, key establishment, signatures, authentication, and the external attack surface an adversary or an auditor sees first. That map is the raw material for the cryptographic bill of materials the new memorandum asks for, alongside the harvest-now exposure view, the algorithm dependency register, the certificate and key risk view, and the executive risk record.

QStrike demonstrates what that exposure means under forward-threat assumptions, on real

hardware, in terms a board will act on, and without touching a client's production keys. QSolve turns the evidence into a funded, sequenced migration plan with named owners. Qtonic Quantum Lab scores independently what a vendor claims is quantum-safe, so readiness is verified rather than assumed.

The case for this firm rests on claims you can check. Qtonic Quantum sells no cryptography, no hardware, and no migration stack of its own, so the inventory has no thumb on the scale. QScout maps findings against 15 compliance frameworks and treats the inventory as a living record, which is the exact posture the federal guidance now normalizes, so readiness holds as standards move rather than expiring with the report.

QSCOUT FIELD SIGNAL

100,000+	cryptographic findings cataloged
5,000+	High or Critical exposures identified
2,300+	exposures addressed
100+	governed engagements
0	production incidents

Field evidence corpus available for customer review under NDA.

> **The founders kept an inventory of every secret they held. The 250th year is a good one to run yours.**

FIND IT BEFORE YOU FIX IT

Every migration that succeeds begins in the same place, with a map of where you are exposed. The direct path is a scoped cryptographic discovery assessment, and the Y2Q briefing explains what it covers and where it starts.

Start a scoped discovery assessment

DEVIL'S ADVOCATE

Anniversary marketing is a fair charge, and so is timeline skepticism. Google's 2029 date is not a prediction of Q-Day, and no public machine breaks RSA or elliptic-curve cryptography at scale today. Grant all of it. The market is not waiting for proof of collapse. Google, Cloudflare, and Microsoft have moved their own timelines. France has moved certification. The United States has moved federal migration. OMB has moved the work into inventories, owners, budgets, and plans. A cryptographic inventory also pays for itself on weak keys and expired certificates alone, whatever the quantum clock does. The birthday is the occasion. The procurement cycle is the argument.

Find. Prove. Fix.

---

1. George Washington's Revolutionary War intelligence operations, including the Culper Ring organized under Benjamin Tallmadge in 1778, used a numbered code book of more than 700 entries in which 711 designated Washington, long-held cover identities, dead drops, and the sympathetic stain developed by James Jay. See the public histories maintained by the Central Intelligence Agency and by George Washington's Mount Vernon.

2. Benedict Arnold conducted his correspondence with British intelligence officer John André in cipher. André was captured in September 1780 carrying the plans of West Point, and the plot failed through interception of the courier rather than through cryptanalysis.

3. Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, November 1976. The RSA cryptosystem was described the following year.

4. Peter Shor's algorithm for factoring and discrete logarithms on a quantum computer was published in 1994. NIST finalized the core post-quantum standards, FIPS 203, 204, and 205, in August 2024. The migration-timing framing follows the widely cited analysis associated with Michele Mosca.

5. The French certification guidance was reported by Reuters on June 16, 2026. The US executive order "Securing the Nation Against Advanced Cryptographic Attacks" was signed June 22, 2026, setting a December 31, 2030 milestone for key establishment and December 31, 2031 for digital signatures, with an implementing OMB memorandum placing a migration-planning deadline on federal agencies in late October 2026. Microsoft announced its accelerated 2029 goal for critical products and services on June 30, 2026, via the Microsoft Security Blog ("Accelerating the quantum-safe timeline," June 30, 2026), identifying inventory and discovery as the primary challenge and naming certificate issuance, code signing, key protection, and update pipelines among the most complex areas of its transition. OMB memorandum M-26-15, "Execution of the Migration to Post-Quantum Cryptography," was issued June 2026 (whitehouse.gov) and sets the inventory, CBOM, migration-plan, owner, funding, and monitoring requirements described above.

6. Cloudflare has published an ongoing post-quantum series, including its stated goal of full post-quantum protection by 2029. Meta Engineering described deploying hybrid post-quantum key exchange on internal traffic in May 2024, citing the harvest-now-decrypt-later rationale. Google enabled hybrid post-quantum key exchange by default in Chrome in 2024 and published a post-quantum migration timeline targeting 2029 (blog.google).

7. Engagement and findings figures are drawn from the Qtonic Quantum field corpus, available for customer review under NDA. Public operating-record figures appear in Qtonic Quantum marketplace and standards materials, including the company's post-quantum readiness benchmark release of May 8, 2026, and its platform announcement of March 24, 2026.

8. July 4, 2026 marked the 250th anniversary of the Declaration of Independence.

9. Science-layer references are resource estimates and theoretical architectures, not demonstrated attacks. Google Quantum AI published a lowered resource estimate for attacking elliptic-curve cryptography (research.google, 2025-2026). A Caltech-led group published a theoretical architecture suggesting Shor's algorithm could reach cryptographic scale with fewer physical qubits than earlier models assumed. Neither establishes that a cryptographically relevant quantum computer exists or that any specific arrival date is fixed.

Forward-looking timelines and quantum-arrival estimates are engineering estimates, not predictions of fact. Descriptions reflect the cited materials and public reporting available as of July 2, 2026.

Qtonic Quantum Corp is a quantum risk and vulnerability intelligence firm. Its platforms and advisory services help enterprises and government agencies reach post-quantum readiness and sustain it continuously, as standards, threats, and infrastructure evolve. Qtonic Quantum is vendor-neutral by design, scoring and recommending what works rather than what a vendor sells. Headquartered in Miami, with operations in Be'er Sheva, Israel. Find. Prove. Fix.

QTONIC QUANTUM CORP

Miami, FL
+1 (866) 4-QTONIC
info@qtonicquantum.com · qtonicquantum.com