

— A TECHNICAL & STRATEGIC INVESTMENT BRIEFING

The Quantum *Arsenal*

Military power is still counted in soldiers, aircrafts and dollars. In the twenty-first century, **infrastructure is the defining factor.**

An exploration of capital allocation across applications of quantum technology relevant to modern warfare.

IN THIS SERIES

01: POST-QUANTUM CRYPTOGRAPHY

02: SENSING

03: COMPUTATIONAL FLUID DYNAMICS

04: NAVIGATION

The advantage is purchased *years in advance.*

In modern warfare, **intelligence** increasingly governs the outcome of a conflict. Not merely in winning conflicts, but in averting them, and in preventing the **slow erosion of a state's sovereignty**. Russia, by every conventional metric of military power, should have taken Ukraine in a matter of weeks. Yet, four years on, Kyiv still holds. That resilience was relies on information rather than resilience. Warned by U.S. intelligence weeks before the first missiles fell, Ukraine dispersed its air force and denied Moscow the surprise its entire plan depended on. And **a warning that arrives early enough does more than shape a war**: it can raise the cost of starting one.

In the years since, American targeting data has turned a modest arsenal into a precision instrument. From 2022 a covert pipeline ran space-based intelligence directly into Ukrainian command centers. That intelligence compressed sensor-to-shooter times to minutes, provided advance warning, located Russian hardware, troop mobilization, command posts and the Black Sea fleet. In October that dependence was put to the test. For two nights U.S. early warning of Russian ballistic launches never reached Kyiv, and SpaceX throttled the Starlink terminals on Ukraine's interceptor drones without notice. With no warning, no Patriots and most of its interceptor drones grounded, Kyiv lost all three of its combined heat and power plants in a single night.

Cheap precision munitions have since spread to every arsenal; continuous space-based targeting has not, and the powers that operate it now trade it like ammunition (Washington Post, 2026; SZR via Ukrinform, 2025). The satellites, signals architecture and analytic infrastructure behind it were the product of decades of American investment, funded long before anyone knew the wars they would decide.

SOVEREIGN CAPITAL

The advantage in any conflict is purchased years in advance, by a state willing to fund a capability whose payoff it cannot yet specify. Quantum sits where satellite reconnaissance sat in the 1950s: expensive, immature, and strategically decisive for whoever commits. That bet is being placed again now.

The state has stepped in to make sure the technology matures on sovereign ground. On 21st of May the U.S. Commerce Department announced nine letters of intent totalling \$2.013 billion in CHIPS and Science Act incentives, conditioned on the Department taking a minority, non-controlling equity stake in each company (Department of Commerce, 2026), and on June 22nd a package of executive orders set a government-wide quantum program in motion, including federal PQC migration of high-value systems.

The earlier issue, *Quantum Shadows*, explored quantum's defense applications and how the current war theater has pushed the urgency of their development and procurement. The landscape is rapidly shifting, and since its release we have received plenty of questions around the physics and engineering behind these applications. Therefore, these subsequent Quantum Arsenal issues aim to tackle some of those questions with a designated memo for each technology answering the following: What is the foundation of the technologies, do they deserve capital, on what timeline, at what entry point, and what evidence would prove each bet wrong.

What we are currently seeing in the Quantum defense landscape is analogous to the first radar-equipped aircraft over the English Channel in 1940. Radar existed before the Battle of Britain, but the battle proved it. Thus changing worldwide procurement decisions within months. Quantum defense is approaching its radar moment.

The map of *this issue*.

Executive Overview

02

The advantage is purchased years in advance.

Memo One • Post-Quantum Cryptography

04

I. The Physics	04
II. Shor’s Algorithm Beat Analogy	05
III. The Status	06
IV. The Companies	07
V. The Position	09
VI. The Falsifier	10

For the Average Investor

10

The rare technology bet that needs no breakthrough to pay.

References

11

PUBLICATION

The Quantum Arsenal,
The Intelligence Wars,
Issue IV,
October 2026

SevenTrain Ventures
seventrainventures.com/Quantum

DISCLOSURES

For informational purposes only. Does not constitute investment advice. SevenTrain Ventures holds a position in PsiQuantum, one of the companies discussed in this series. For qualified investors only.

Vikal Kapoor | Founding Partner
Mats Løkebø | Quantum Investment Lead & Operating Partner
Nicholas Schaefer | Research Intern, Quantum Information Science

Post-quantum *cryptography*.

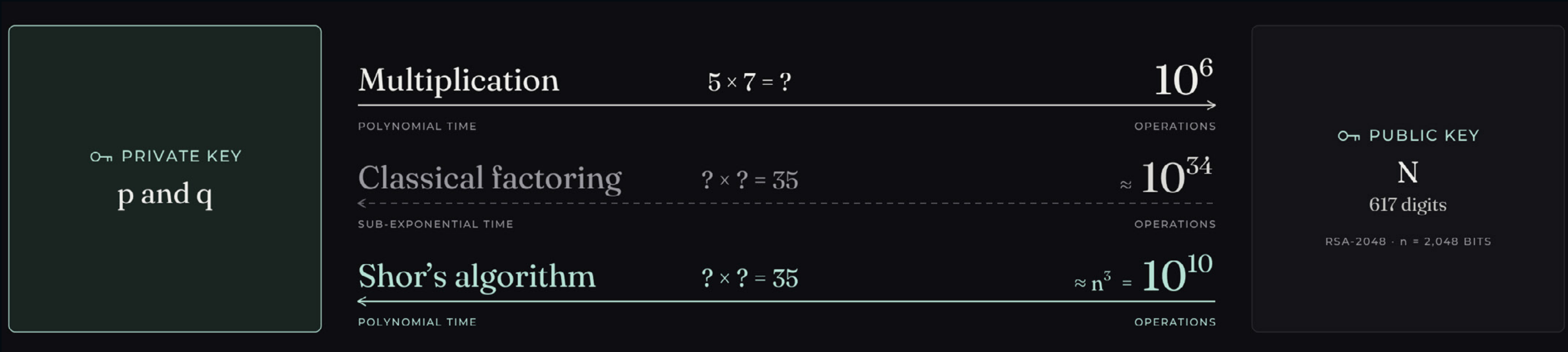
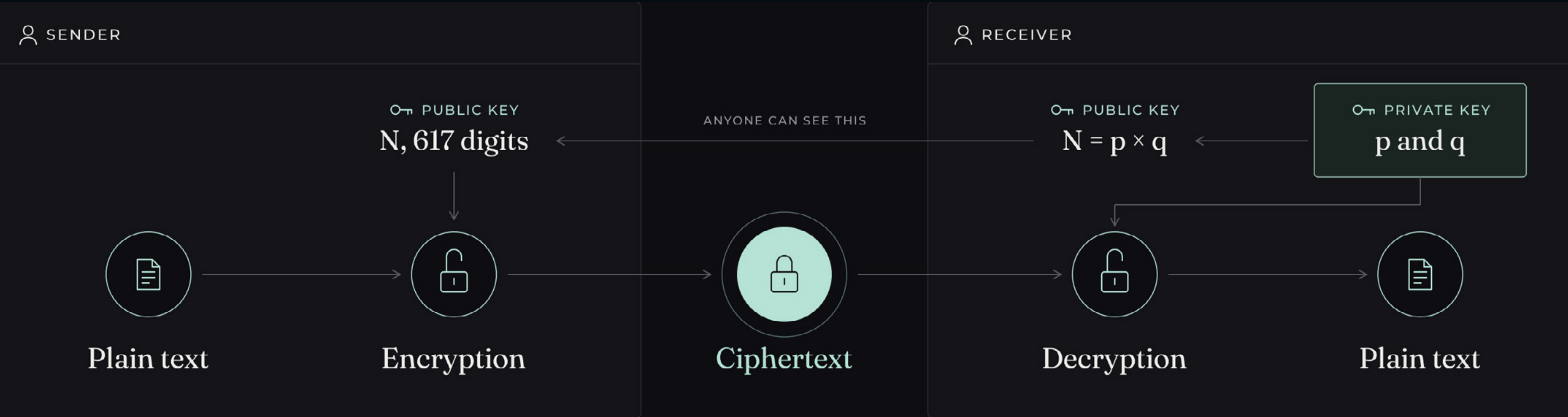
The Physics

TRL	HORIZON	Sample companies	TIMELINE
9 • classical software	Mandated market	PQShield • QuSecure	Now to 2035 • regulator-written

The encryption protecting most of the world’s secure traffic (RSA-2048 and elliptic curve) is currently under threat. This encryption works by “scrambling” the data using a public key. To read the message on the other end, the receiver must “unscramble” it using the private key. Therefore this encryption is secure as long as no one else has the private key. The genius of this method is in the asymmetry of the math; multiplying the private key primes is easy, whereas recovering the private key from the public key is effectively intractable.

Factoring to recover the private key primes from the public key product is a problem that would keep every computer on Earth busy for Millions of Years.

The security of this method of encryption is based on the assumption that the factoring problem is too large to be solved. That assumption holds up when approached using traditional computers. Shor, however, noticed that factoring hides an easier problem if one takes a quantum approach.



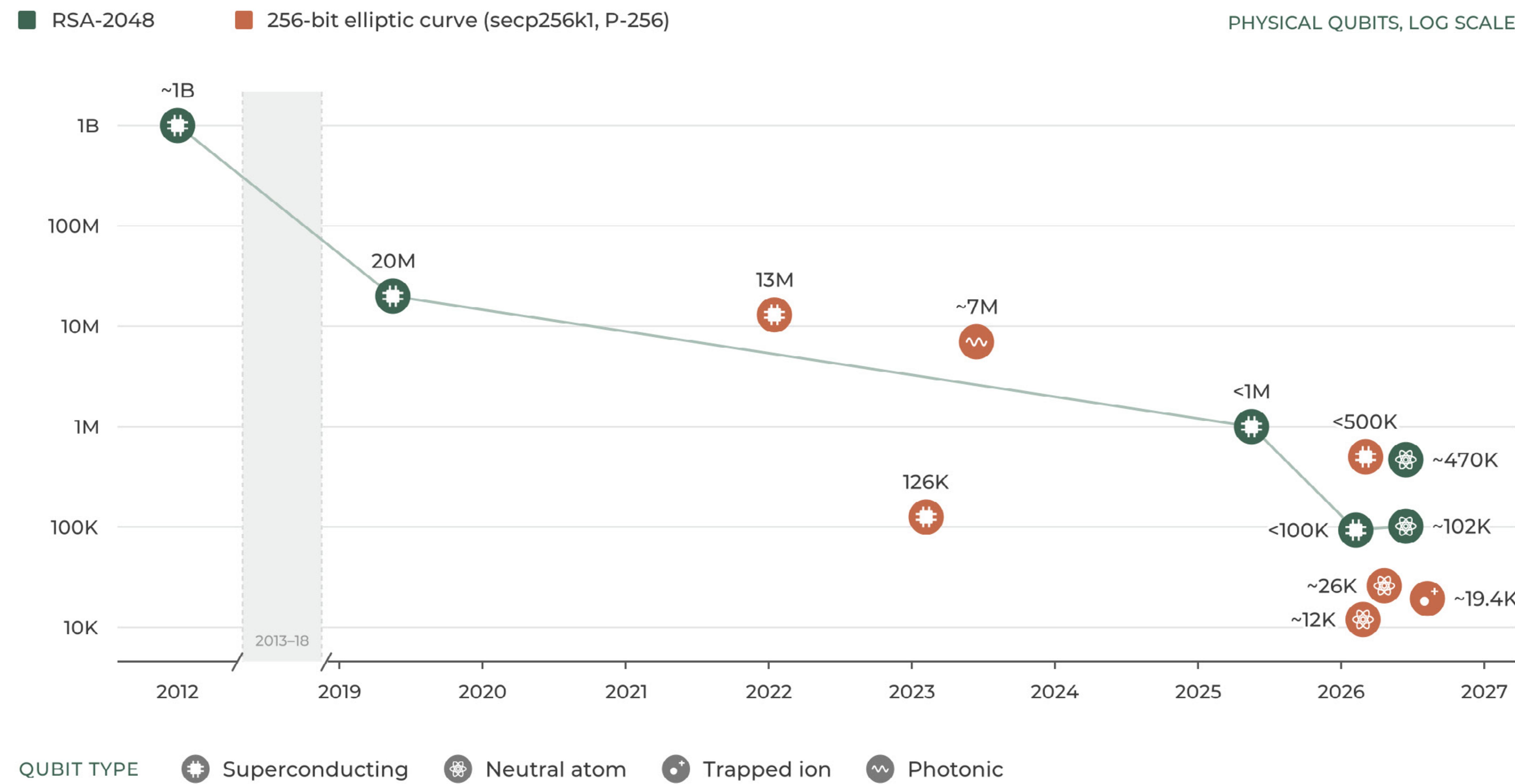
Shor’s algorithm

Shor found the problem has a hidden rythm. His method starts by creating a noisy pattern by raising a random number to higher and higher powers, dividing by the public key each time, and recording the remainder. With enough observations the remainder starts to repeat, like a drum beat. The length of the pattern is called the period, and once you have it, the primes are easily found with a greatest common divisor. Classically you would have to listen to the drum for an astronomical number of beats to find the pattern. A quantum computer does not listen beat by beat. It holds every possible exponent

in superposition, produces the whole drum line at once, and runs a quantum Fourier transform to pull the rhythm out from the noise: this cancels each wrong tempo, adds up the right one, and eventually reads out the period.

Today’s quantum hardware does still not have this capability, but the requirements are becoming more attainable as clever new approaches develop. Anything encrypted and recorded today will be readable once a cryptographically relevant machine exists. More on what constitutes a cryptographically relevant machine below.

FIG. 03 · THE FALLING ESTIMATE
Number of qubits required to break encryption



RUNTIMES SPAN MINUTES TO 264 DAYS. QUBIT TYPES DIFFER. POINTS ASSUME DIFFERENT HARDWARE SPECIFICATIONS. 2026 POINTS ARE PREPRINTS.
SOURCES: FOWLER 2012; GIDNEY & EKERÅ 2019; WEBBER 2022; GOUZIEN 2023; LITINSKI 2023; GIDNEY 2025;

Cryptographically relevant machines are still years out. What has changed is how far. Measured in qubit-days (qubits × runtime), the cost of breaking RSA-2048 has fallen roughly 99% since 2012. Most of that gain came before 2019. In 2019 [Gidney](#) put the attack at 20 million noisy qubits and 8 hours. In May 2025 [Gidney](#) cut that to under a million on the same physical assumptions, a gain from better arithmetic and

error correction, yet most of the improvement was paid for in time; from 8 hours to 5 days. In qubit-days that is about 30% cheaper, as opposed to the twentyfold suggested by the headline.

The 2026 publications headlining even lower qubit counts are mostly time-space tradeoffs rather than drastic cost improvements. Cain’s 10,000 qubit neutral atom

configuration takes 264 days of continuous operation to break ECC-256; the 26,000-atom version of the same design brings that to 10 days. The market is still watching qubit roadmaps. They do not show the hardware quality the estimates assume: error rates, decoder speed, coherence over days of uninterrupted operation.

Fault tolerance and cryptographic relevance are separate thresholds. [IBM's Starling](#) (2029) and [QuEra's Libra](#) (2028) will be genuinely useful machines, and neither threatens RSA. The best public machines today yield about [50 to 100](#)

logical qubits. The estimates require 1,200 to 1,450 at drastically lower error rates, faster decoding and longer coherence. The largest elliptic-curve key anyone has actually broken on quantum hardware is a mere [15 bits](#).

[The Global Risk Institute](#) now puts a cryptographically relevant machine within ten years at 28% to 49%, up from 19% to 34% the year before. Mass-scale cryptographically relevant machines remain distant. Recent results show they are closer than previously thought.

[EXECUTIVE ORDER 14412](#), SEC. 1, JUNE 2026

“...the risk of adversaries collecting United States information now, and decrypting it later once large-scale quantum computers are operational.”

HNDL

Harvest now, decrypt later is the security industry's name for an attack of nationally consequential proportion already in process today. An adversary recording encrypted communications need not break them today; it keeps them until a machine that can is built. The bet rests on the assumption that a fault tolerant quantum computer (FTQC) arrives within the useful lifetime of the data being collected. [CNSA 2.0](#) names that collection as the reason for the migration timeline and treats it as active (NSA, 2022).

The Status

The standards development phase has passed. The migration now runs on commodity algorithms and procurement deadlines. NIST finalized [FIPS 203](#), [204](#) and [205](#) in August 2024 and picked [HQC](#) as the backup key-encapsulation mechanism in March 2025. [CNSA 2.0](#) requires quantum-resistant algorithms in new national-security systems from 2027, exclusive use in networking equipment by 2030, and full migration by 2035. [EO 14412](#), signed in June, sets 31 December 2030 for post-quantum key establishment and 31 December 2031 for signatures on federal high-value systems, with a proposed FAR rule extending the 2030 date to covered contractors. OMB's implementing memo, [M-26-15](#), requires every agency to file a migration plan by 22 October 2026, run [TLS 1.3](#) by January 2030, and build an automated cryptographic inventory that feeds a bill of materials.

Budgets are already moving with the estimates. [Google](#) set a 2029 migration deadline in March 2026. [Cloudflare](#) followed in April. [Microsoft](#) pulled the completion date of its Quantum Safe Program forward from 2033 to 2029. [CISA's January buying list](#) already tells agencies to purchase only post-quantum-capable cloud, messaging, browsers and disk encryption; networking, identity and operating systems are next.

Corporate migration has already begun. **Chrome** and **Edge** use [hybrid ML-KEM by default](#). [OpenSSH](#) has shipped post-quantum key exchange as its default since 2022. **Apple** moved iMessage to [PQ3](#) and Signal moved to [POXDH](#). **OpenSSL 3.5**, the library under most of the internet's TLS, has had [hybrid ML-KEM on by default](#) since April 2025. **AWS** turned on [hybrid ML-KEM for KMS, Certificate Manager and](#)

[Secrets Manager](#) in April 2025, with every HTTPS endpoint to follow. **Microsoft** shipped [ML-KEM and ML-DSA](#) into Windows 11, Windows Server 2025 and .NET 10 in November 2025, in the crypto API applications already call.

By April 2026 [over 65%](#) of human traffic reaching Cloudflare used post-quantum key agreement. Nobody has deployed post-quantum certificates on the web: an ML-DSA certificate chain is about twelve times the size of today's, Chrome has said it has no plan to add such certificates to its root store,

but [the replacement](#) it is building with Cloudflare is scheduled for a quantum-resistant root store in late 2027.

This capability is more urgent than most investors assume. Every sensitive system and communications network has to move to post-quantum encryption. Newly standardized PQC algorithms are believed to be secure from quantum attacks, but new methods could render them obsolete. Thus this field, just like the rest of the cybersecurity industry, will likely experience cat-and-mouse style adaptations.



The Companies

The biggest names in PQC are incumbents: Thales, IBM, Palo Alto Networks and the hyperscalers. All of them can bundle migration into existing contracts and take the revenue without being re-rated for it. [Palo Alto shipped that in January](#): inventory, risk scoring and a proxy that re-encrypts legacy traffic to ML-KEM, inside the firewall subscription. What incumbents cannot build fast enough, they buy.

FIG. 04
Acquisitions in cryptographic security

DATE	ACQUIRER	TARGET	FOCUS	VALUE
MAY 2025	Keyfactor	InfoSec Global, CipherInsights	Discovery and agility; then raised \$1B+	Undisclosed
MAY 2025	IonQ	ID Quantique	Swiss QKD vendor; majority stake, reported value	~\$250M
OCT 2025	Cadence	Secure-IC	Embedded security and PQC silicon IP	Undisclosed
FEB 2026	Palo Alto Networks	CyberArk	Including Venafi, bought 2024 for \$1.54B	\$25B
MAR 2026	AppViewX	Eos	AI-agent identity, next to its PKI products	Undisclosed
JUL 2026	Keyfactor	Cofide	Workload and AI-agent identity; agreed, not yet closed	Undisclosed
SEP 2026	Project Eleven	Riva Labs	Post-quantum signatures and wallets	Undisclosed
OCT 2026	SAIC	Information Security Corp.	PKI vendor on NSA's approved list	Undisclosed
OCT 2026	IonQ	Elisity	Zero-trust identity; agreed, in stock	Up to \$1.3B

This looks to be the beginning of industry' consolidation. Yet one must consider that this recent accusation spree, especially by companies such as IONQ has been largely fuelled by extraordinary public market considitions that opened up cheap funding. This public market frenzy calm down at some point in the next decade. In that scenario the M&A activity is likely to slow down with it. Regardless, acquisition is a probable exit for such specialist companies.

QuSecure

PRODUCT
QuProtect

APPROACH
Network-layer PQC, no
application rewrites

CONTRACTING
Phase III SBIR · GSA MAS ·
MDA SHIELD

LATEST
\$3.9M AFWERX TACFI award,
Jan 2026

QuSecure sells network-layer software, QuProtect, that finds an organization's cryptography and moves live traffic to the NIST post-quantum algorithms by policy, with no application rewrites and a fallback to classical TLS. It is the only PQC vendor with a [Phase III SBIR](#), which lets agencies buy sole-source, and its product sits on [GSA's Multiple Award Schedule](#). A [\\$3.9 million AFWERX TACFI award](#) in January 2026 funds the push for IL6 authorization of

QuProtect with Air Force Global Strike Command, with classified-cloud deployment targeted for Q3 2026, and the company holds a seat on the [Missile Defense Agency's SHIELD vehicle](#), which has over 2,400 awardees and pays only through competed task orders. QuSecure's strength lies in government capture with contracting authority. That is a curcial differentiating capability when most of the technology is commoditized.

PQShield

MODEL
Licensed PQC IP for silicon and
firmware

REVENUE 2025
£2.3M, up 536%

FUNDING
\$37M Series B, June 2024

FOUNDED
2018, by Ali El Kaafarani

PQShield sells post-quantum cryptography as licensed IP: software libraries and hardware cores that chipmakers and equipment vendors build into their own silicon and firmware (Microchip, AMD, Lattice and STMicro are named partners). [Audited revenue](#) rose 536% to £2.3 million in 2025, 89% of it licenses at 56% gross margin, with multi-year U.S. contracts signed in late 2025 still to come through. Its staff and advisers co-authored every NIST PQC standard published so far, and

its PQCryptoLib library is one of few that carries [FIPS 140-3 certification](#). The [\\$37 million Series B](#) in June 2024, led by Addition, priced it as an IP company: its cryptography ships inside other companies' silicon and firmware, a specialist position the platforms cannot bundle away.

The team: Ali El Kaafarani, an Oxford Mathematical Institute researcher, founded the company in 2018, and the team has had an active role in developing the NIST post-quantum standards

evolutionQ

PRODUCT
BasejumpQDN

MODEL
Key management for
quantum-safe networks

FUNDING
US\$5.5M Series A, 2022

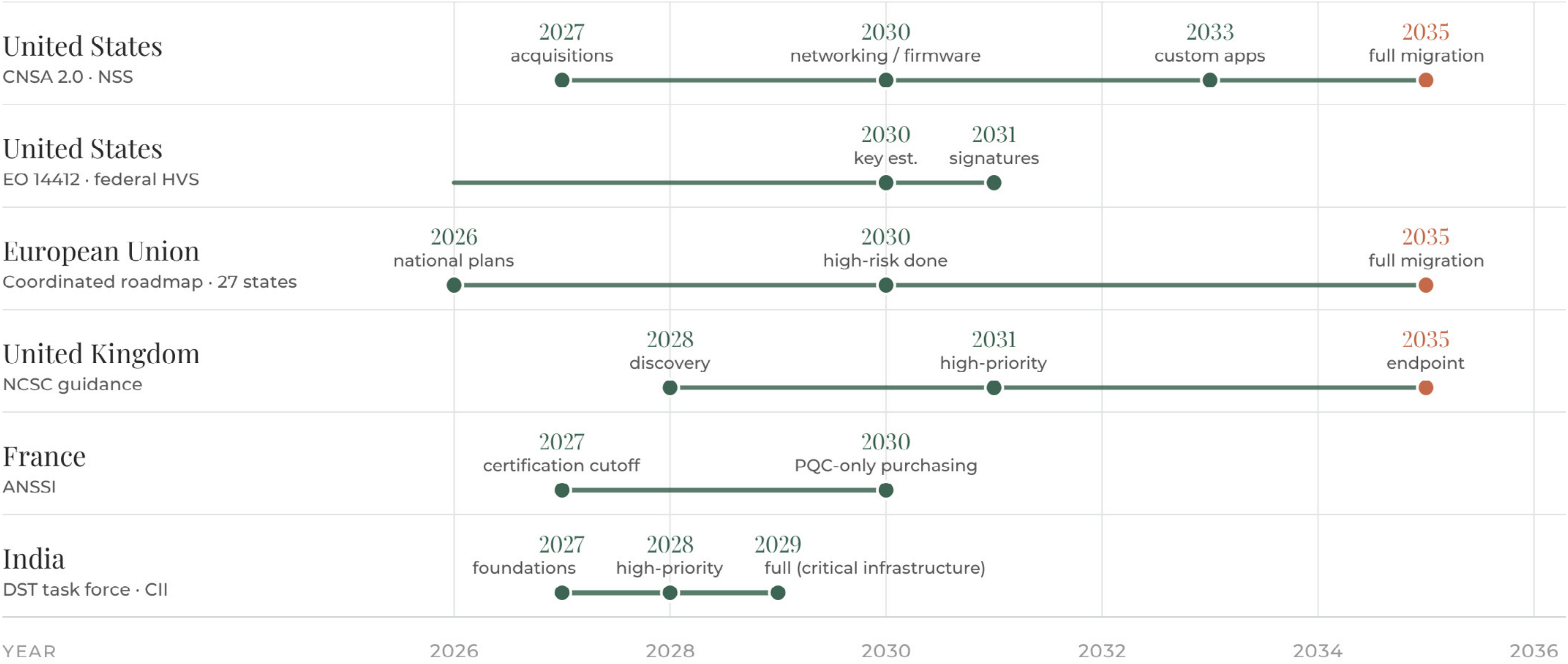
ROOTS
Waterloo's Institute for
Quantum Computing

evolutionQ sells the software that manages a quantum-safe network's keys. BasejumpQDN takes keys from any vendor's QKD hardware and from PQC and routes them across fiber and satellite links, so an operator adds quantum-safe links without replacing the network. It runs [Kirq](#), the public QKD network from Sherbrooke to Quebec City, where Nokia, Honeywell and Crypto4A validated a critical-infrastructure blueprint on it in February 2026, and the Bank of Canada hired it for quantum-safe digital-currency design.

The team: Their lab lineage is canonical. Michele Mosca co-founded Waterloo's Institute for Quantum Computing, the lab the rest of this industry recruits from, and writes the [Global Risk Institute's threat timeline](#), the survey the sector quotes. Co-founder Norbert Lütkenhaus runs IQC today, and co-founder David Jao is chief cryptographer. [Quantonation](#) led its US\$5.5 million Series A in 2022, which SandboxAQ joined. Although their technology is world class, it is not clear that QKD will provide enough value to justify its complexity and cost.

FIG. 05 · SIX SCHEDULES

Government mandated PQC migration timelines



DATES AS PUBLISHED, OCTOBER 2026. NCSC AND THE EU ROADMAP ARE GUIDANCE, NOT STATUTE.

The Position

Certified implementations below the platform.

The algorithms are free, so nobody pays for ML-KEM. They pay for a validated module that runs it inside a chip, a radio or a weapons system, and for the people who can get it validated. A FIPS 140-3 validation took about 348 days in January and only a handful of certificates list ML-KEM, so a vendor holding one sells into a queue. The platforms cannot bundle what sits below them in silicon.

Contracting authority in defense.

The 2027 national-security gate and the 2030 to 2031 federal dates are fixed, the money arrives through sole-source vehicles and task orders, and no platform can buy its way into a Phase III SBIR.

Arqit rose 35% the trading day after the executive order was signed, showing that companies in this industry reprice on migration-deadline announcements as well as on procurement contracts.

RISKS

01 Commoditization

The algorithms are free and the platforms bundle.

02 Deadline drift

[NIST IR 8547](#), which carries the 2030 and 2035 dates, is still a draft; [CISA's product list](#) came seven weeks late; [GAO](#) found in October that none of the 24 CFO Act agencies met all three basic practices. The [Senate's FY27 defense bill](#) might mitigate the drift.

Either condition is enough. If the CNSA 2.0 or EO 14412 deadlines are materially relaxed, or if migration collapses into a feature of incumbent platforms, visible as awards going to integrators while specialists lose out, the captive-market premium disappears and the thesis reverts to ordinary cybersecurity exposure.

WHERE TO WATCH

- | | | |
|--|------------------------------|---|
| 01 Agency migration plans to OMB (22 October deadline) | 02 Federal awards on SAM.gov | 03 CMVP and Common Criteria certificate lists |
| 04 CNSA 2.0 FAQ revisions | 05 The FY27 NDAA conference | 06 M&A activity |

For the Average Investor

The encryption protecting your bank, your hospital records and military communications is expected to fall to a quantum computer eventually. We do not know when, but for this bet it does not matter: Every U.S. system of any national-security interest must migrate by 2030 to 2035 regardless. Thus the winners are those who hold certified IP in silicon and contracting authority in defense.

HNDL is active.
The mitigators
hold the certificates
& relationships

For More Information

Feel free to contact our team to discuss this memo or our other work in quantum.

CONTACT

Mats Løkebø

QUANTUM INVESTMENT LEAD & OPERATING PARTNER

mats@seventrainventures.com
seventrainventures.com/quantum



DISCLOSURES

For informational purposes only. Does not constitute advice to purchase or sell any securities. SevenTrain Ventures holds a position in PsiQuantum, one of the companies discussed in this series. For qualified investors only.

Vikal Kapoor | Founding Partner
Mats Løkebø | Quantum Investment Lead & Operating Partner
Nicholas Schaefer | Research Intern, Quantum Information Science

PUBLICATION

The Quantum Arsenal,
The Intelligence Wars,
Issue IV,
October 2026

SevenTrain Ventures
seventrainventures.com/Quantum

References

Peer-reviewed sources, standards, and primary program and contract announcements underlying the claims in this issue. Company and contract entries are primary press or government releases; technical claims are sourced to the peer-reviewed literature.

SOVEREIGN CAPITAL & INTELLIGENCE

- [1] Entous, A. (2025). The partnership: The secret history of the war in Ukraine. The New York Times, 29 March 2025.
- [2] The Washington Post. (2026). Russia is providing Iran intelligence to target U.S. forces, officials say (6 March 2026).
- [3] Ukrinform. (2025). Foreign Intelligence Service of Ukraine (SZR) officer Oleh Alexandrov on Chinese satellite reconnaissance data supplied to Russia for missile strikes [interview, 4 October 2025].
- [4] U.S. Department of Commerce. (2026). CHIPS incentives: nine letters of intent totalling \$2.013 billion, including seven quantum computing companies [press release, 21 May 2026].
- [5] Ukrainian Air Force, via Ukranews. (2026). Russia launches nearly 40 ballistic missiles and over 100 drones at Ukraine (15 October 2026).
- [6] Euronews. (2026). Starlink terminals operations restricted in Ukraine overnight, adviser to Zelenskyy says (14 October 2026).
- [7] CNN, via Censor.net. (2026). Ukraine has completely run out of Patriot missiles to intercept ballistic missiles (15 October 2026).
- [8] Ukrainian Air Force, via Ukranews. (2026). Russia launches nearly 40 ballistic missiles and over 100 drones at Ukraine (15 October 2026).
- [9] Euronews. (2026). Starlink terminals operations restricted in Ukraine overnight, adviser to Zelenskyy says (14 October 2026).
- [10] CNN, via Censor.net. (2026). Ukraine has completely run out of Patriot missiles to intercept ballistic missiles (15 October 2026).

ALGORITHMS & RESOURCE ESTIMATES

- [11] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Computing, 26(5), 1484–1509.
- [12] Barker, E. (2020). Recommendation for key management: Part 1, General (NIST SP 800-57 Part 1, Rev. 5). National Institute of Standards and Technology.
- [13] Fowler, A. G., Mariantoni, M., Martinis, J. M., & Cleland, A. N. (2012). Surface codes: Towards practical large-scale quantum computation. Physical Review A, 86, 032324.

- [14] Gidney, C., & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5, 433 (arXiv:1905.09749, 2019).
- [15] Gouzien, É., Ruiz, D., Le Régent, F.-M., Guillaud, J., & Sangouard, N. (2023). Performance analysis of a repetition cat code architecture: Computing 256-bit elliptic curve logarithm in 9 hours with 126 133 cat qubits. *Physical Review Letters*, 131, 040602.
- [16] Litinski, D. (2023). How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates. arXiv:2306.08585 (PsiQuantum).
- [17] Gidney, C. (2025). How to factor 2048-bit RSA integers with less than a million noisy qubits. arXiv:2505.15917.
- [18] Webster, P., et al. (2026). The Pinnacle Architecture: Reducing the cost of breaking RSA-2048 to 100 000 physical qubits using quantum LDPC codes. arXiv:2602.11457 (Iceberg Quantum).
- [19] Cain, M., et al. (2026). Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits. arXiv:2603.28627.
- [20] Babbush, R., Zalcman, A., Gidney, C., Broughton, M., Khattar, T., Neven, H., Bergamaschi, T., Drake, J., & Boneh, D. (2026). Securing elliptic curve cryptocurrencies against quantum vulnerabilities: Resource estimates and mitigations. arXiv:2603.28846.
- [21] Schrottenloher, A. (2026). Optimized point addition circuits for elliptic curve discrete logarithms. IACR ePrint 2026/1128.
- [22] Häner, T., et al. (2026). Computing 256-bit elliptic curve discrete logarithms in 26 days on a fault-tolerant trapped-ion quantum computer with 20,000 qubits. IACR ePrint 2026/1916 (IonQ).
- [23] Dasu, S., DeCross, M., Guo, A. Y., et al. (2026). Computing with many encoded logical qubits beyond break-even. arXiv:2602.22211 (Quantinuum Helios).
- [24] Project Eleven. (2026). Q-Day Prize awarded for the largest quantum attack on elliptic curve cryptography to date: a 15-bit key [press release, 24 April 2026].
- [25] Global Risk Institute. (2025). Quantum threat timeline report 2025 (Mosca, M., & Piani, M.; published March 2026).
- [26] IBM. (2025). Roadmap to large-scale fault-tolerant quantum computing: Starling, 2029 [blog, June 2025].
- [27] QuEra Computing. (2026). Libra, a 2028 fault-tolerant quantum computer, and expanded AWS collaboration [press release, 15 June 2026].

STANDARDS, POLICY & DEADLINES

- [28] National Institute of Standards and Technology. (2016). Report on post-quantum cryptography (NIST IR 8105).
- [29] National Institute of Standards and Technology. (2024). FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA).

- [30] National Institute of Standards and Technology. (2024). Transition to post-quantum cryptography standards (NIST IR 8547, initial public draft, November 2024).
- [31] National Institute of Standards and Technology. (2025). NIST selects HQC as fifth algorithm for post-quantum encryption [news release, 11 March 2025].
- [32] National Security Agency. (2022; updated 2025). Commercial National Security Algorithm Suite 2.0 (CNSA 2.0).
- [33] National Security Agency. (2024). CNSA 2.0 frequently asked questions, version 2.0 (April 2024).
- [34] The White House. (2025). Executive Order 14306, Sustaining select efforts to strengthen the Nation's cybersecurity and amending Executive Order 13694 and Executive Order 14144 (6 June 2025). Federal Register, FR Doc. 2025-10804.
- [35] The White House. (2026). Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks (22 June 2026). 91 FR 38483.
- [36] Office of Management and Budget. (2026). M-26-15: Execution of the migration to post-quantum cryptography (24 June 2026).
- [37] Office of Management and Budget & Office of the National Cyber Director. (2024). Report on post-quantum cryptography: \$7.1 billion federal civilian migration estimate, 2025 to 2035.
- [38] Cybersecurity and Infrastructure Security Agency. (2026). Product categories for technologies that use post-quantum cryptography standards (23 January 2026).
- [39] National Security Agency. (2026). NSA announces post-quantum cryptography measures to safeguard national security systems against quantum computing threats [press release, 1 October 2026].
- [40] Government Accountability Office. (2026). Quantum computing: Federal actions needed to prepare for emerging cyber threat (GAO-27-108740, 6 October 2026).
- [41] U.S. Senate. (2026). FY2027 National Defense Authorization Act, Sec. 1631: post-quantum cryptography deadlines for the Department of Defense [as summarized in the BSA conference letter, 27 August 2026].
- [42] ANSSI. (2026). Certification of security products without quantum-resistant encryption to end from 2027 [announced 16 June 2026; as reported by Reuters, 16 June 2026, and The Quantum Insider, 18 June 2026].
- [43] NIS Cooperation Group / European Commission. (2025). Coordinated implementation roadmap for the transition to post-quantum cryptography (23 June 2025).
- [44] UK National Cyber Security Centre. (2025). Timelines for migration to post-quantum cryptography (20 March 2025).
- [45] Department of Science and Technology, India. (2026). Quantum-safe ecosystem in India: task force report (May 2026).

[46] National Institute of Standards and Technology, CMVP. (2026). Cryptographic Module Validation Program queue status: average of 348 days for the last 30 validations [January 2026 update, as reported by PostQuantum.com, 21 September 2026].

[47] National Institute of Standards and Technology, CMVP. (2024). Certificate #4800: PQCryptoLib (PQShield), FIPS 140-3 (16 September 2024).

DEPLOYMENT

[48] Google. (2024). A new path for Kyber on the web [Google Security Blog, 13 September 2024].

[49] Cloudflare. (2026). Post-quantum cryptography support: hybrid ML-KEM default in Chrome 131+ and Edge 131+ [developer documentation].

[50] OpenSSH. (2022). OpenSSH 9.0 release notes: hybrid post-quantum key exchange by default.

[51] Apple. (2024). iMessage with PQ3: The new state of the art in quantum-secure messaging at scale [Apple Security Research, February 2024].

[52] Signal. (2023). Quantum resistance and the Signal Protocol [Signal blog, 19 September 2023].

[53] OpenSSL. (2025). OpenSSL 3.5.0 final release: ML-KEM, ML-DSA and SLH-DSA, hybrid ML-KEM default in TLS [release notes, 8 April 2025].

[54] Amazon Web Services. (2025). ML-KEM post-quantum TLS now supported in AWS KMS, ACM and Secrets Manager [AWS Security Blog, April 2025].

[55] Microsoft. (2025). Post-quantum cryptography APIs now generally available on Microsoft platforms [Microsoft Security Community blog, November 2025].

[56] Google. (2026). Quantum frontiers may be closer than they appear [blog, 25 March 2026; sets the 2029 post-quantum migration timeline].

[57] Cloudflare. (2026). Cloudflare targets 2029 for full post-quantum security [blog, 7 April 2026; source of the 65% of human traffic figure].

[58] Microsoft. (2026). Microsoft advances quantum-safe security as the risk timeline shifts [Microsoft Security Blog, 30 June 2026].

[59] Ivezic, M. (2026). Google's Merkle Tree (MTC) gambit to quantum-proof HTTPS. PostQuantum.com, 28 February 2026 [analysis of the Chrome Security blog post "Cultivating a robust and efficient quantum-safe HTTPS", 27 February 2026].

[60] Bernstein, D. J., et al. (2025). KyberSlash: Exploiting secret-dependent division timings in Kyber implementations. CHES 2025.

[61] Bernstein, D. J. (2026). Exploiting ML-DSA bugs. cr.yp.to, 1 June 2026.

MARKET, DEALS & COMPANIES

[62] MarketsandMarkets. (2025). Post-quantum cryptography market forecast to 2030.

[63] Mordor Intelligence. (2025). Post-quantum cryptography market, 2025 to 2030.

[64] Palo Alto Networks. (2026). Introducing Quantum-Safe Security [blog, 27 January 2026].

[65] CyberArk. (2024). Completion of the acquisition of Venafi [press release, October 2024].

[66] Palo Alto Networks. (2026). Palo Alto Networks completes acquisition of CyberArk [press release, 11 February 2026].

[67] Keyfactor. (2025). Acquisitions of InfoSec Global and CipherInsights [press release, 13 May 2025].

[68] Keyfactor. (2026). Strategic growth investment of more than \$1 billion led by Summit Partners [press release, 6 July 2026].

[69] Keyfactor. (2026). Agreement to acquire Cofide [as reported by Biometric Update, 27 July 2026].

[70] Cadence Design Systems. (2025). Cadence completes acquisition of Secure-IC [press release, 30 October 2025].

[71] IonQ. (2025). IonQ completes acquisition of ID Quantique [press release, 6 May 2025]; BNN Bloomberg (25 February 2025) on the reported value of about US\$250 million.

[72] AppViewX. (2026). AppViewX acquires Eos [press release, 19 March 2026].

[73] Project Eleven. (2026). Project Eleven acquires Riva Labs [press release, 29 September 2026].

[74] SAIC. (2026). SAIC acquires Information Security Corporation [press release, 5 October 2026].

[75] IonQ. (2026). IonQ to acquire Elisity [press release, 12 October 2026].

[76] QuSecure. (2022). SBIR Phase III federal procurement contract for post-quantum cybersecurity [press release, 29 June 2022].

[77] QuSecure. (2023). QuProtect available via GSA Multiple Award Schedule [press release, 14 September 2023].

[78] QuSecure. (2026). QuSecure selected for SBIR TACFI contract award to deliver IL6 PQC capabilities to Air Force Global Strike Command [press release, 4 March 2026; award dated 15 January 2026].

[79] QuSecure. (2026). Position on the Missile Defense Agency SHIELD IDIQ [press release, 25 February 2026].

[80] U.S. Department of War / Missile Defense Agency. (2026). SHIELD IDIQ third tranche of awards; pool exceeds 2,400 awardees [announcement, 15 January 2026].

- [81] PQShield. (2022). PQShield algorithms to be standardized as NIST announces first international standards for post-quantum cryptography [press release, 5 July 2022].
- [82] PQShield. (2024). \$37 million Series B led by Addition [press release, 20 June 2024].
- [83] PQShield. (2026). UltraPQ Suite upgrades at Embedded World; collaboration with STMicroelectronics alongside Microchip and Lattice [press release, 10 March 2026].
- [84] PQShield Ltd. (2026). Annual report and financial statements for the year ended 31 December 2025. Companies House, filed 6 August 2026.
- [85] Quantonation. (2022). evolutionQ secures US\$5.5 million in Series A funding for global expansion [press release, 13 June 2022].
- [86] evolutionQ & Numana. (2024). Kirq, the first public-access quantum-safe network in Québec, is powered by evolutionQ's BasejumpQDN [press release, 10 June 2024].
- [87] Nokia. (2026). Nokia, Numana and partners validate quantum-safe network Blueprint 7 to secure Canada's critical infrastructure [press release, 24 February 2026].
- [88] evolutionQ. (2023). Bank of Canada engages evolutionQ in research on quantum-safe digital currencies [press release, 2023].
- [89] Arqit Quantum. (2026). Select preliminary financial results for the second half and full fiscal year 2026 [press release, 8 October 2026].
- [90] Kishor, N. (2026). Arqit Quantum (NASDAQ:ARQQ) jumps 35.57% as US quantum orders ignite a security rally. Kalkine, 24 June 2026 [close of \$29.04 on 23 June 2026].