

QUANTA SECURITY AND ENCRYPTION



Twelve perspectives on the state, applications, and trajectory of quantum security — from cryptographic fundamentals to Golden Dome and the decade ahead.
Quanta Diplomacy • Quantum Security Briefing • August 2026

CONTACT

Quanta Diplomacy

info@quantadiplomacy.org

Phone number: (704) 219-0176

<https://www.quantadiplomacy.org/>

Introduction to Quantum Security

Why a computing revolution has become a national-security problem.

Quantum security is the set of technologies and practices built to protect information and systems in a world where quantum computers exist. It has two faces. The defensive face is post-quantum cryptography (PQC): new mathematical schemes designed to resist attack by quantum computers, replacing algorithms like RSA and elliptic-curve cryptography that quantum methods can eventually break. The offensive or enabling face is quantum-based capability itself — quantum sensing, quantum timing, and quantum communication — which can be used to detect, navigate, and communicate in ways classical technology cannot match.

The core threat comes from two quantum algorithms. Shor's algorithm can efficiently factor large numbers and solve discrete-logarithm problems, undermining RSA and elliptic-curve cryptography — the backbone of most internet and government encryption today. Grover's algorithm speeds up brute-force search against symmetric encryption, effectively halving the strength of schemes like AES-128. Adversaries can already engage in “harvest now, decrypt later” collection — storing encrypted data today with the intent of decrypting it once a capable quantum machine exists.

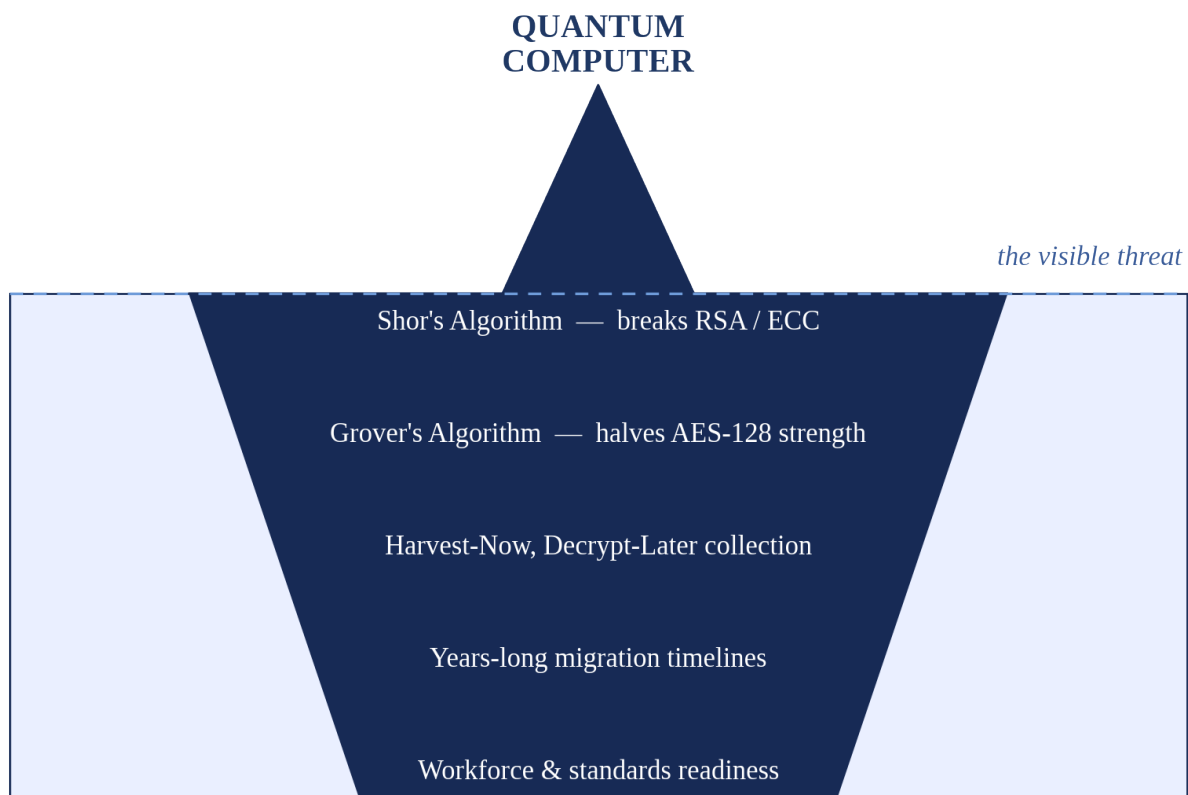


Figure 1. The cryptographic threat runs deeper than a single algorithm — it runs through the full stack.

Quantum Security in the USA and UK

Two allied approaches converging on the same timeline.

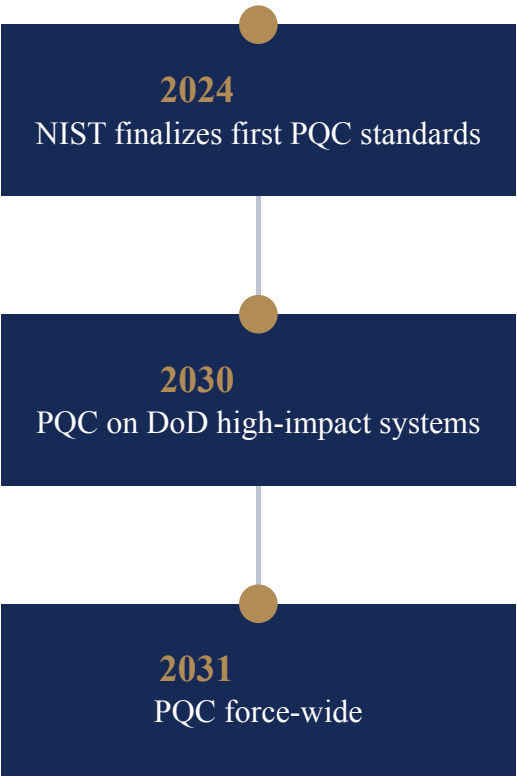
United States

U.S. policy runs on two tracks. NIST finalized its first PQC algorithm standards in 2024, following selection of four candidate algorithms in 2022. On defense policy, the Department of War published a Post-Quantum Cryptography Strategy requiring quantum-resistant cryptography on high-impact systems by 2030 and across the entire force by 2031. A June 2026 executive order elevated quantum computing, sensing, and networking as a unified national technology priority.

United Kingdom

The UK's National Cyber Security Centre (NCSC) has taken a phased regulatory approach: define migration goals by 2028, complete early high-priority migration by 2031, and finish PQC migration nationally by 2035. The NCSC was among the first major national authorities to formally endorse NIST's quantum-safe algorithms.

UNITED STATES



UNITED KINGDOM

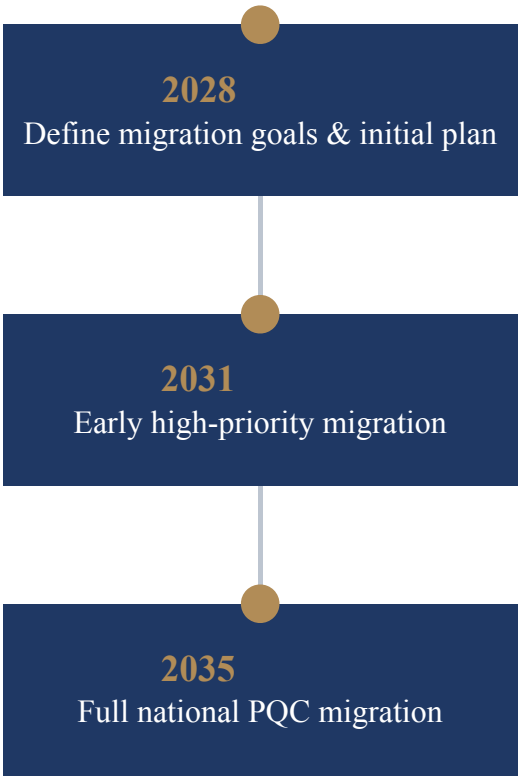


Figure 2. Two allied tracks, converging on the same decade.

Where Quantum Security Is Used in Golden Dome

The homeland missile-defense shield's quantum-dependent layers.

Golden Dome for America is designed as a layered, multi-domain shield against ballistic, hypersonic, and cruise-missile threats, integrating satellites, radars, interceptors, and command centers across space, land, sea, and air. Quantum technologies enter the program in three main places: positioning, navigation, and timing (PNT) — optical atomic clocks and quantum inertial sensors that reduce dependence on jammable GPS; sensing and tracking — quantum RF sensors aimed at maneuverable hypersonic threats classical radar struggles against; and secure, resilient communications — post-quantum cryptography protecting the sensor-to-shooter data chain across every domain.



Figure 3. Three quantum-enabled pillars underpin the Golden Dome architecture.

How Golden Dome Is Supported by Quantum Technology

Clarifying the relationship — there is no separate “Quantum Dome” program.

A note on terminology: research did not turn up a distinct program called “Quantum Dome.” What exists is quantum technology functioning as a supporting layer within Golden Dome itself, not a separate parallel system.

Golden Dome is explicitly described by its own contractors and analysts as depending on next-generation fields — space technology, AI, and quantum communication — to achieve the systems-integration goals the program sets out. Quantum sensing and timing supply the PNT backbone so interceptors and sensors can operate coherently without relying solely on GPS. Quantum-resistant cryptography protects the sensor-to-shooter data chain against both current interception and future quantum decryption. R&D investment in quantum technologies is framed — similarly to the Apollo program's civilian spillover — as producing dual-use benefits beyond missile defense.

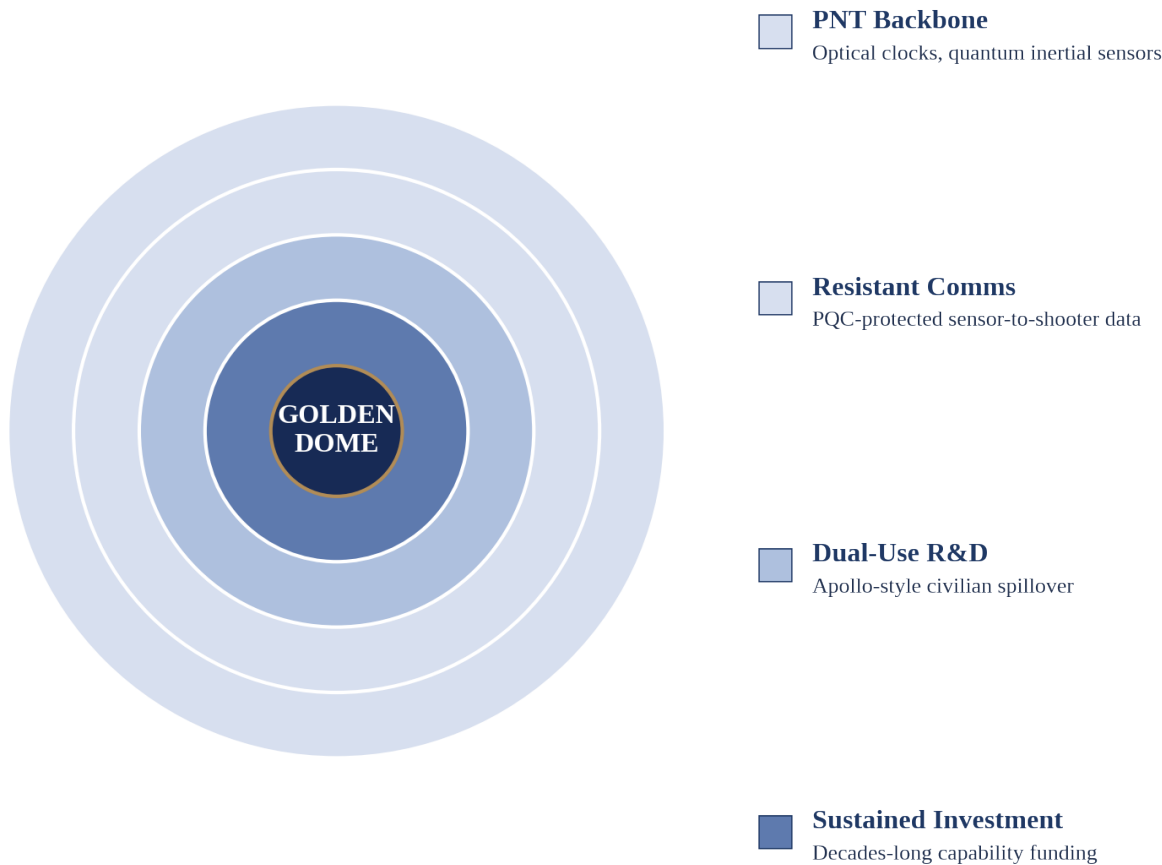


Figure 4. Golden Dome at the core, with four quantum-enabled supporting layers.

Quantum Security and Encryption

From vulnerable classical schemes to lattice-based standards.

The encryption side of quantum security is dominated by the shift to post-quantum cryptography (PQC) — algorithms built on mathematical problems believed to remain hard even for quantum computers. The leading category is lattice-based cryptography (e.g., Kyber for key encapsulation), alongside code-based and multivariate-polynomial approaches. NIST selected its first four PQC algorithms in July 2022 and published draft standards for three of them in August 2023. The UK NCSC recommends hybrid cryptography — running classical and post-quantum algorithms side by side — to smooth the transition.

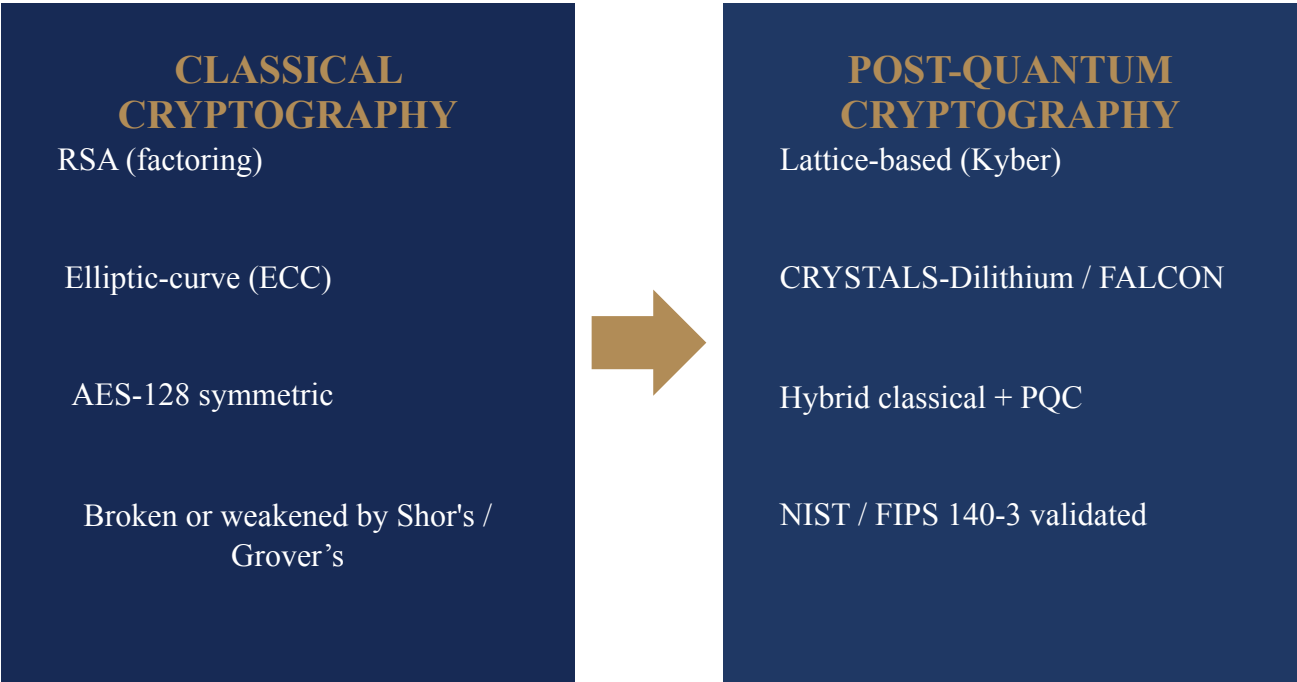


Figure
5. The migration from classical to post-quantum cryptography.

Quantum Security and Tackling the Threat

Migration frameworks, crypto-agility, and the adversary picture.

MITRE's Post-Quantum Cryptography Migration Roadmap, published through the PQC Coalition, breaks the transition into four stages. A recurring theme across MITRE, NCSC, and industry guidance is crypto-agility: designing systems so cryptographic algorithms can be swapped without re-architecting the underlying system. MITRE researchers estimate that a quantum computer capable of breaking RSA-2048 is unlikely before roughly 2055–2060 absent major breakthroughs, though some experts believe advances in error correction could pull that forward to around 2035.

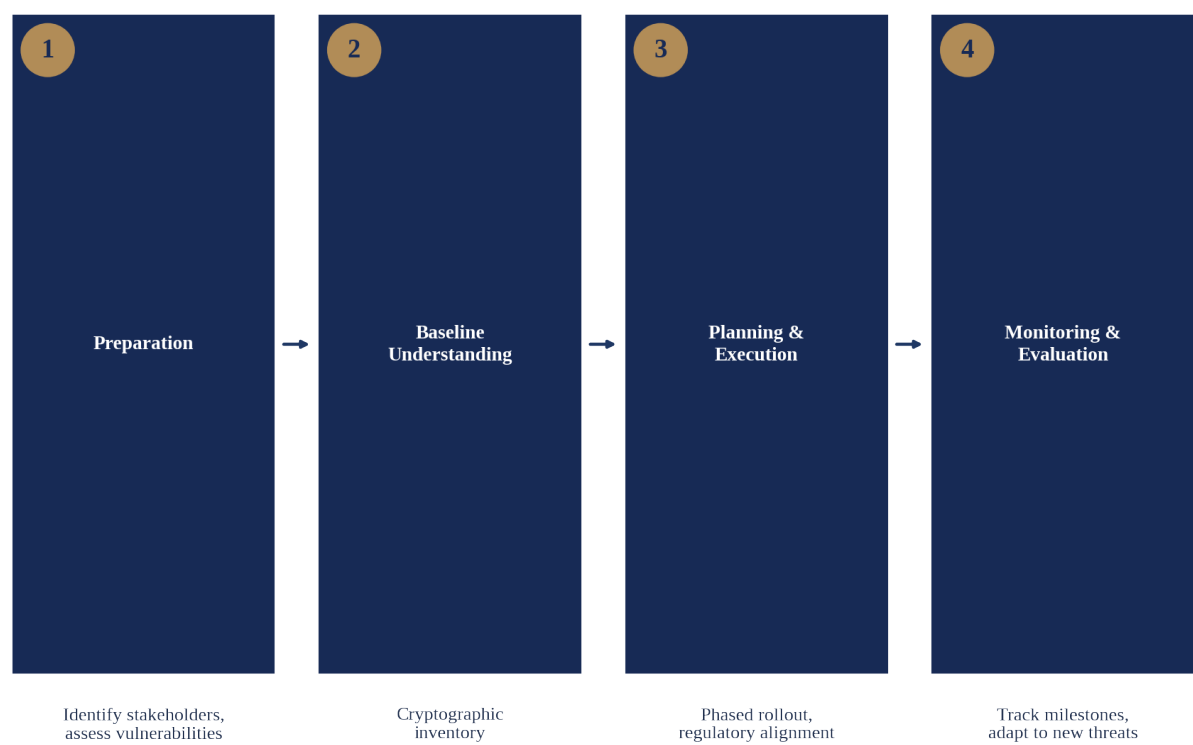


Figure 6. The four-stage PQC migration process.

Raytheon (RTX) Quantum Security Leadership

Sensor integration, networking, and cryptography for defense communications.

Raytheon's quantum-security position rests on combining its sensor and communications integration expertise with BBN Technologies' quantum networking research. Industry analysis describes RTX as developing quantum-enhanced radar and electronic-warfare capabilities and as active in post-quantum cryptography migration across military communications systems. A 2021 strategic collaboration agreement with IBM aims to jointly develop artificial intelligence, cryptographic, and quantum solutions for aerospace, defense, and intelligence customers.



Figure 7. Raytheon's quantum-security portfolio spans four focus areas.

Northrop Grumman Quantum Security Leadership

Building quantum hardware while flagging the risks it creates.

Northrop Grumman occupies both sides of the quantum-security equation. On the build side, the company is developing Reciprocal Quantum Logic (RQL) — a superconducting chip technology cooled near absolute zero, enabling precise, high-speed control of electrical currents without the dense cabling that normally limits how large quantum systems can scale. On the risk side, reporting tied to the company's space-systems work has been explicit about “Q-Day” — the point at which a sufficiently powerful quantum computer breaks conventional encryption — pointing to incidents like the 2022 Viasat cyberattack and a European Space Agency data breach as evidence that distance and orbit no longer provide inherent security.

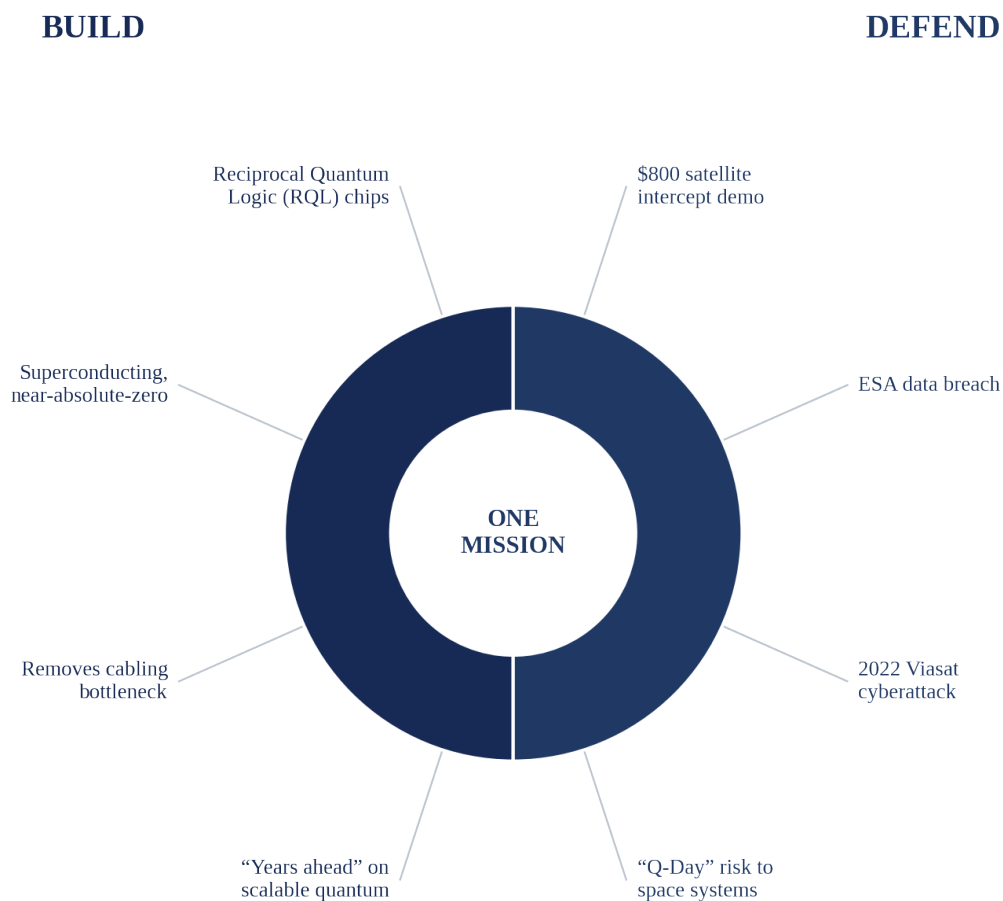


Figure 8. Northrop Grumman's dual role: building quantum capability, defending against quantum risk.

MITRE Quantum Security R&D

Coalition-building, migration guidance, and the “Quantum Moonshot.”

MITRE co-founded the PQC Coalition in September 2023 alongside IBM Quantum, Microsoft, PQShield, SandboxAQ, and the University of Waterloo. By 2025 the coalition had grown to more than 125 contributing organizations and released its PQC Migration Roadmap. MITRE's internal “Quantum Moonshot” initiative develops hardware and protocols across four areas: unconditionally secure quantum communications, quantum sensing, post-quantum cryptography, and universal photonic quantum computing, with AI integrated throughout.

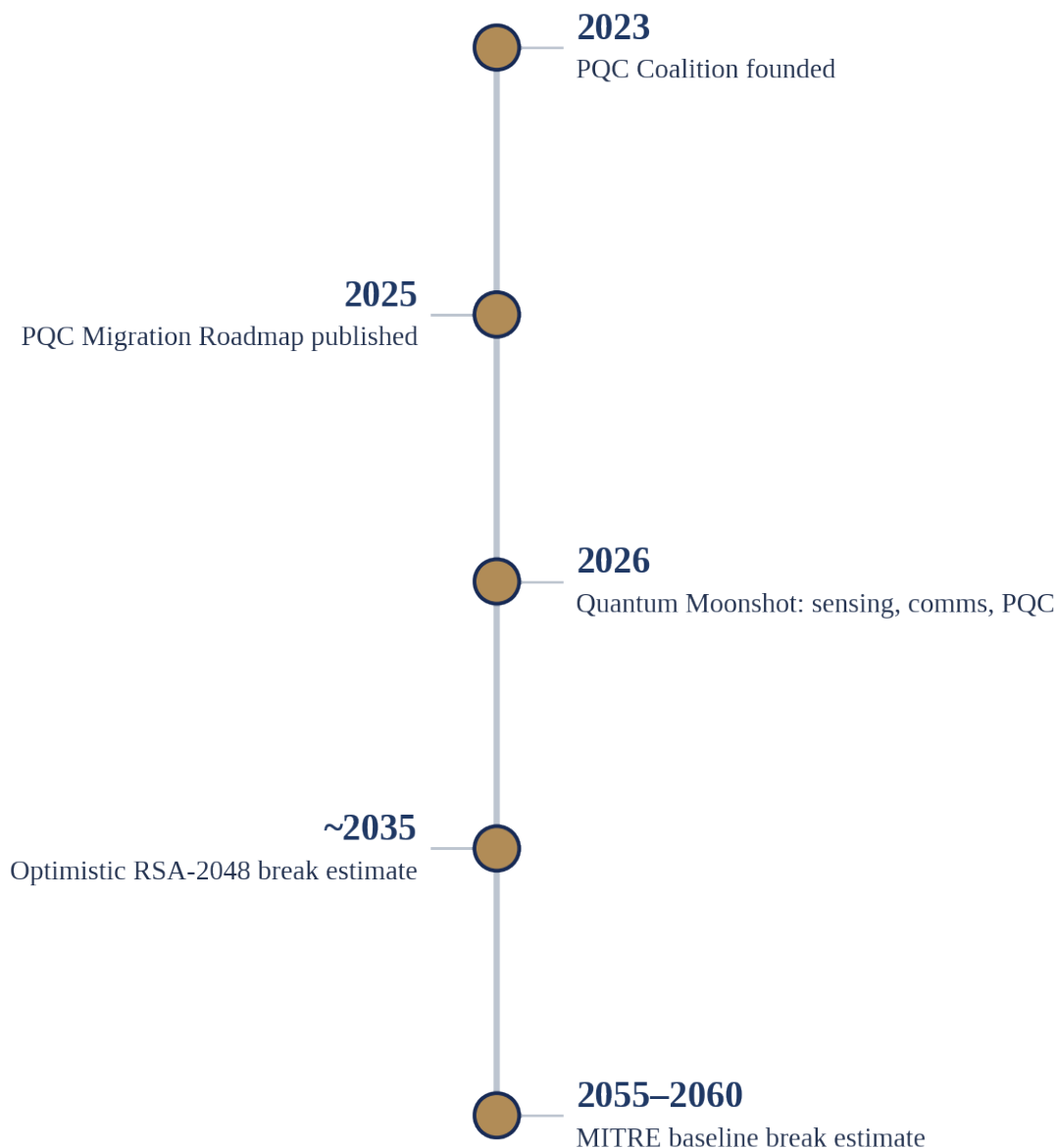


Figure 9. MITRE's coalition timeline and threat-estimate range

Defense Innovation Unit (DIU) Quantum Security

Fielding quantum sensing and timing at operational speed.

Launched in 2024, DIU's Transition of Quantum Sensors (TQS) program focuses on positioning, navigation, timing, and anomaly detection. Field testing began in early 2025, and in July 2025 DIU partnered with the Air Force Rapid Capabilities Office to fly a strategic-grade quantum inertial sensor aboard the X-37B spaceplane. In June 2026, DIU launched Project Farseer, a roughly \$200 million solicitation authorized under Executive Order 14411, aiming to field mature quantum sensing hardware directly into the operational Joint Force.

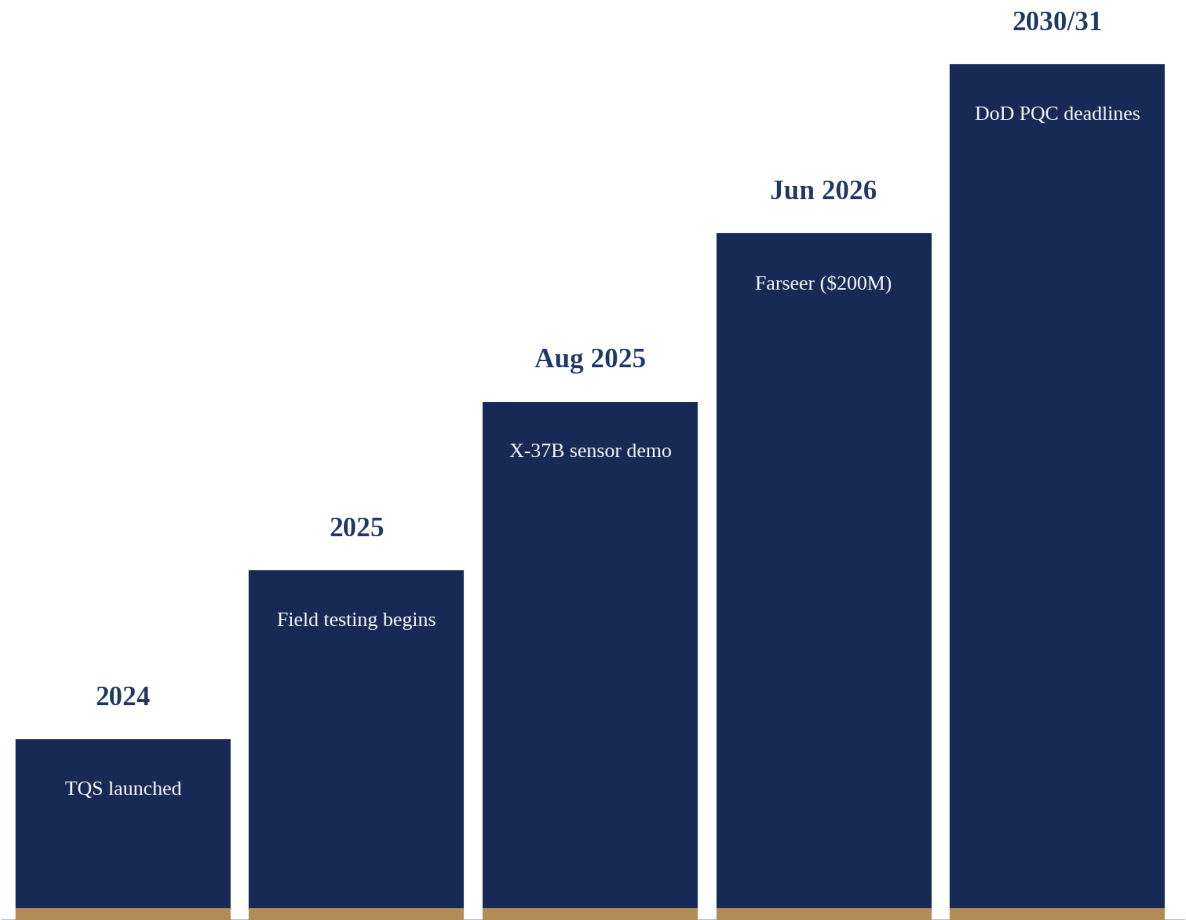


Figure 10. DIU's fielding milestones ascend toward the 2030/31 DoD PQC deadlines.

Recommendations for Improving and Fortifying Quantum Security

Priorities drawn from current guidance and program experience.

- Start cryptographic inventory now — map every system using vulnerable algorithms before setting a migration plan.
- Design for crypto-agility so PQC algorithms can be swapped as standards mature.
- Adopt hybrid cryptography during the transition, as the UK NCSC recommends.
- Treat long-lived sensitive data as already exposed to harvest-now-decrypt-later collection.
- Invest in quantum sensing and timing alongside cryptography — it is maturing faster and delivers near-term value.
- Use public-private coalitions, like the PQC Coalition, to spread cost and expertise.
- Close the workforce skills gap early, not as an afterthought.
- Align allied timelines between the U.S. and UK to standardize procurement and interoperability.



Figure 11. Crypto-agility is the organizing principle behind every recommendation.

The Next Ten Years of Quantum Security

2026–2036: from migration mandates to a quantum-secured baseline.

Over the coming decade, quantum security is likely to move from a specialist compliance topic to a default engineering requirement. DoD's mandate for quantum-resistant cryptography on high-impact systems by 2030 and force-wide by 2031 will likely set the practical pace for the broader U.S. defense industrial base. The UK's 2035 full-migration deadline suggests a staggered but converging allied timeline through the mid-2030s.

Quantum sensing and timing — already ahead of quantum computing in maturity — are likely to see the fastest fielding, with programs like Golden Dome serving as flagship integrators that pull the underlying technology from prototype into operational status.

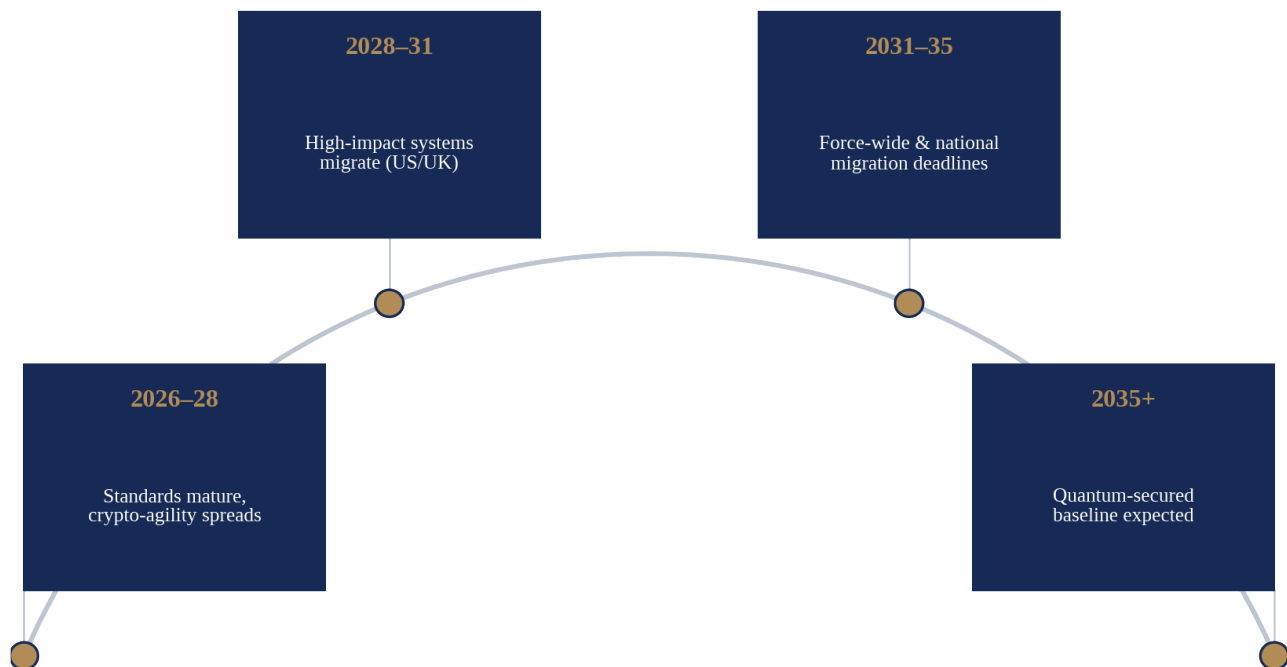


Figure 12. A decade of converging deadlines, from standards maturity to a quantum-secured baseline.