

Q-Day



*Industry Landscape, Thought Leadership, and Policy Recommendations for the United States,
United Kingdom, and NATO*

Manage Defense International

Quantum Security Policy Paper

August 2026

Abstract

Post-quantum cryptography has moved from theoretical concern to active policy question. This paper surveys the industry, academic, and consulting response to “Q-Day” — the point at which a cryptographically relevant quantum computer could break the public-key encryption underlying most digital infrastructure — and evaluates the readiness of the United States, the United Kingdom, and NATO. It finds a young but genuinely capitalized commercial sector, a small number of universities producing the field's foundational research and commercial spin-outs, and a striking consensus among five global consultancies that quantum readiness is a governance issue rather than a purely technical one. The paper concludes with jurisdiction-specific and cross-cutting recommendations centered on cryptographic inventory, timeline alignment among allies, and continued investment in quantum sensing alongside cryptography.

1. Introduction

Two quantum algorithms motivate the modern quantum-security agenda. Shor's algorithm, published in 1994, demonstrated that a sufficiently powerful quantum computer could efficiently factor large integers and solve the discrete-logarithm problem — the mathematical foundations of RSA and elliptic-curve cryptography, which together secure most of today's internet traffic, financial transactions, and government communications. Grover's algorithm compounds the problem by halving the effective strength of symmetric encryption schemes such as AES-128. Neither threat requires a working quantum computer to exist today: adversaries can already engage in “harvest-now, decrypt-later” collection, storing encrypted traffic now with the intention of decrypting it once a capable quantum machine becomes available.

The point at which such a machine exists has become known, somewhat informally, as “Q-Day.” Estimates vary considerably. MITRE researchers place the most likely arrival of a computer capable of breaking RSA-2048 in the 2055–2060 range absent major breakthroughs, while acknowledging that advances in quantum error correction could pull that date forward to as early as 2035. That uncertainty has not slowed policy responses: the U.S. National Institute of Standards and Technology finalized its first post-quantum cryptography standards in August 2024, the U.S. Department of War has set 2030 and 2031 deadlines for migrating high-impact and force-wide systems respectively, and the UK National Cyber Security Centre has published a 2028–2031–2035 migration timeline of its own.

This paper examines the ecosystem that has formed around that migration: the companies building post-quantum cryptography and quantum key distribution products, the universities producing the underlying research, the consultancies advising boards on how to act, and the policy recommendations that follow for the United States, the United Kingdom, and NATO.

2. The Quantum Security Industry Landscape

Before surveying individual companies, a methodological note is warranted. No publicly verifiable ranking of the “top 100” quantum-security companies exists for either the United States or the United Kingdom, and claims to the contrary should be treated with skepticism. The most rigorous industry trackers — Tracxn and The Quantum Insider, among others — identify roughly twenty-seven to forty-four companies in the United States whose core business is quantum-resistant cybersecurity, and a comparable order of magnitude in the United Kingdom. A list padded to one hundred entries per country would necessarily include firms for which quantum security is a marginal feature rather than a core offering. This paper instead presents the most credible and well-documented leaders in each market.

2.1 United States

The U.S. quantum-security market spans three overlapping categories: post-quantum cryptography software and crypto-agility platforms, quantum key distribution hardware, and large security incumbents embedding quantum-safe features into existing product lines. Representative leaders across these categories are summarized in Table 1.

Company	Headquarters	Quantum-Security Focus
<u>Keyfactor</u>	Ohio	Crypto-agility platform that discovers, manages, and rotates certificates and keys through PQC migration.
<u>DigiCert</u>	Utah	Post-quantum-ready digital certificates; publisher of an annual Quantum Readiness Outlook survey.
<u>Entrust</u>	Minnesota	PKI, HSM, and identity vendor integrating post-quantum algorithms into existing certificate infrastructure.
<u>IBM</u>	New York	Quantum hardware alongside PQC contributions to NIST standards (CRYSTALS-Kyber, CRYSTALS-Dilithium).
<u>Palo Alto Networks</u>	California	Quantum-safe capabilities embedded in its Next-Generation Firewall and SASE platforms.
<u>SandboxAQ</u>	California	Alphabet spin-out that raised over \$300 million in December 2024 for cryptographic discovery and PQC migration tooling.

<u>Crypt</u>	New York	Quantum-safe key generation designed to prevent “harvest-now, decrypt-later” attacks.
<u>Quantum Xchange</u>	Maryland	Operator of the Phio quantum key distribution (QKD) network, among the earliest commercial QKD products in the United States.
<u>Quantum Knight</u>	Texas	Embeddable post-quantum cryptographic modules for existing infrastructure.
<u>Patero</u>	Maryland	Hybrid post-quantum network encryption that reduces exposed attack surface for data-in-motion.
<u>QuSecure</u>	California	Software-based, crypto-agile PQC orchestration for government and enterprise networks.
<u>Quantinuum</u>	Colorado	Formed from the merger of Honeywell Quantum Solutions and Cambridge Quantum; combines quantum hardware with cybersecurity applications.
<u>Rambus</u>	California	Semiconductor security intellectual property incorporating post-quantum root-of-trust designs.
<u>AWS (Amazon)</u>	Washington	Hybrid post-quantum TLS already deployed across Amazon Web Services.

Table 1. Representative leaders in U.S. quantum security, by headquarters and focus area.

2.2 United Kingdom

The UK's quantum-security sector is more geographically concentrated than that of the United States, clustering around Oxford and Cambridge university spin-outs, London-based cryptography vendors, and established defense primes. The UK National Cyber Security Centre has been an unusually early and vocal advocate for post-quantum migration, and that advocacy appears to have helped seed a dense cluster of specialist vendors, summarized in Table 2.

Company	Headquarters	Quantum-Security Focus
<u>PQShield</u>	Oxford	Oxford University spin-out that contributed to all three

		NIST PQC standards finalized in August 2024; raised \$37 million in Series B funding.
<u>Post-Quantum</u>	London	Quantum-safe VPN, identity verification, and cryptographic-inventory and migration tooling.
<u>Arqit Quantum</u>	London	Symmetric-key quantum-safe encryption delivered as a cloud service; listed on Nasdaq under ARQQ.
<u>KETS Quantum Security</u>	Bristol	Chip-scale quantum key distribution and quantum random-number generation on photonic chips.
<u>Quantum Dice</u>	Oxford	Oxford spin-out producing self-certifying quantum random-number generators for cryptographic keys.
<u>Crypto Quantique</u>	London	Post-quantum hardware root-of-trust for connected and IoT devices.
<u>Crypta Labs</u>	London	Quantum random-number generation and integrated security chips for mobile and IoT cryptographic applications.
<u>BAE Systems (Quantum)</u>	Hampshire	Quantum sensing, navigation, and communications for defense and security applications.
<u>QinetiQ</u>	Farnborough	UK Ministry of Defence quantum-navigation trials and quantum sensing for aerospace and defense.
<u>Riverlane</u>	Cambridge	Quantum error-correction software (Deltaflow.OS); selected for DARPA's Quantum Benchmarking Initiative.
<u>Oxford Quantum Circuits</u>	Reading	Superconducting quantum computing hardware, part of the wider Oxford quantum cluster.
<u>Cavero Quantum</u>	Leeds	University of Leeds spin-out producing lightweight post-quantum cryptography for

		constrained IoT devices.
--	--	--------------------------

Table 2. Representative leaders in UK quantum security, by headquarters and focus area.

Both ecosystems remain young relative to the scale of the migration task ahead of them. DigiCert's 2026 Quantum Readiness Outlook, surveying more than one thousand IT and security decision-makers across the United States, the United Kingdom, and Australia, found that eighty-seven percent of organizations report planning, testing, or implementing post-quantum cryptography, yet only seven percent have deployed quantum-safe cryptography at scale. That gap between stated intention and actual deployment motivates much of the recommendations set out in Section 5.

3. Thought Leadership on Q-Day

Academic thought leadership on Q-Day is concentrated in a small number of institutions, each of which has translated research into applied commercial or governmental capability rather than remaining purely theoretical.

3.1 University of Oxford



Oxford co-hosts the Oxford Post-Quantum Cryptography Summit together with the UK National Cyber Security Centre at the university's Mathematical Institute. It is also home to [POShield](#), an Oxford spin-out and, by its own account, the largest concentration of post-quantum cryptographers under one roof anywhere in the world, heavily involved in the NIST standardization process. Oxford further anchors a broader quantum-hardware cluster — including [Oxford Ionics](#) and [Oxford Quantum Circuits](#) — adjacent to the National Quantum Computing Centre at Harwell.

Quantum research hub: <https://nqcc.ac.uk>

3.2 University of Cambridge

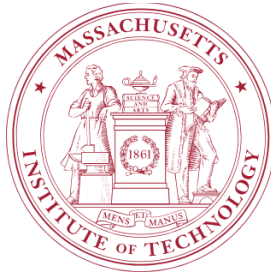


UNIVERSITY OF CAMBRIDGE

Cambridge's Centre for Quantum Information and Foundations originated the field of relativistic quantum cryptography and remains a core member of the UK Quantum Communications Hub. In March 2026, Cambridge and [IonQ](#) launched the IonQ Quantum Innovation Centre at the Cavendish Laboratory, a facility explicitly scoped to include quantum security and communications research alongside quantum computing.

Quantum department: <https://www.qi.damtp.cam.ac.uk>

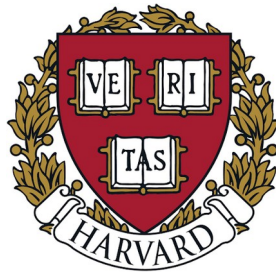
3.3 Massachusetts Institute of Technology



MIT's Quantum Initiative, a Presidential Initiative led by faculty director Danna Freedman, organizes the university's quantum work around five pillars — computing, sensing, simulation, materials, and networks — with security and encryption named as a direct application area. MIT's Center for Quantum Engineering has produced more of the field's dissertations and publications than any other American institution, and the university partners with [MIT Lincoln Laboratory](#) to move quantum-security research toward national-security deployment.

Quantum department: <https://quantum.mit.edu>

3.4 Harvard University



The Harvard Quantum Initiative is constructing a dedicated quantum science and engineering facility at 60 Oxford Street and has launched one of the first doctoral programs in the field. Harvard and MIT researchers have jointly demonstrated a quantum-repeater node that addresses signal loss, described by the researchers as the missing link toward a practical, secure quantum internet, and Harvard participates in three of the five Quantum Information Science Research Centers announced by the Department of Energy and the White House Office of Science and Technology Policy.

Quantum department: <https://quantum.harvard.edu>

3.5 Stanford University



Stanford's Q-FARM initiative — Quantum Fundamentals, Architecture, and Machines — directed by Patrick Hayden and Jelena Vučković, connects Stanford's and SLAC's theoretical and experimental quantum science programs. Stanford ranks third nationally by quantum dissertations and publications, providing a deep pipeline of researchers into post-quantum cryptography and quantum security more broadly.

Quantum department: <https://qfarm.stanford.edu>

4. Thought Leadership Among Global Consultancies

Five global consultancies have published the most widely cited quantum-security guidance directed at boards and chief executives, and their published work converges on a shared conclusion, addressed further in Section 6.

4.1 Accenture



Accenture operates a dedicated Quantum Security practice that helps clients prepare for quantum-era encryption threats and plan post-quantum cryptography migration.

Quantum security practice:

<https://www.accenture.com/us-en/services/emerging-technology/quantum-security>

4.2 KPMG



KPMG publishes a Quantum Readiness framework spanning cryptographic discovery, risk prioritization, and migration roadmaps across its UK, U.S., and Swiss practices. In 2026 the firm co-authored a white paper with the Hong Kong Monetary Authority assessing banking-sector quantum readiness, and its board-guidance article “Prepare Now for Quantum Cyber Risk” frames Q-Day explicitly as a matter of board-level governance and disclosure rather than a purely technical concern.

Quantum security practice:

<https://kpmg.com/us/en/capabilities-services/advisory-services/cyber-security-services/cyber-strategy-governance/kpmg-q-prep-postquantum-cryptography-readiness.html>

4.3 McKinsey



McKinsey's "Quantum cybersecurity: Preparing for Q-Day and PQC" argues that quantum readiness is a leadership priority requiring a cross-functional group spanning technology, risk, and business leadership. The firm reports that quantum-technology investment grew from two billion dollars in 2024 to thirteen billion dollars in 2025, a sixfold year-over-year increase that it attributes to growing confidence in the commercial viability of quantum technologies.

Quantum security practice: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/quantum-is-almost-here-are-you-and-your-systems-ready>

4.4 Booz Allen Hamilton



Booz Allen Hamilton, the leading provider of artificial-intelligence and cybersecurity services to the U.S. federal government, operates a dedicated Quantum Information Science and Technology practice under Vice President JD Dulny. The firm has expanded its venture-capital investment, through Booz Allen Ventures, in the quantum-hardware company [SEEQC](#) to accelerate quantum engineering for national-security missions, and it sponsored an independent report from the [Center for Strategic and International Studies](#) proposing ways to strengthen federal cybersecurity, including provisions addressing quantum risk.

Quantum security practice: <https://www.boozallen.com/insights/ai/quantum-s-potential-to-unlock-finance-insights.html>

4.5 Bain & Company



Bain announced a strategic collaboration with [IBM](#) in 2026 to deliver post-quantum cryptography risk assessments to private-equity and corporate clients, framing quantum computing explicitly as a threat to proprietary data and intellectual property during due-diligence and holding periods — a framing distinct from, though complementary to, the national-security emphasis of the other four firms surveyed.

Quantum security practice: <https://www.bain.com/insights/how-businesses-can-prepare-for-post-quantum-cybersecurity-threats/>

5. Policy Recommendations by Jurisdiction

The recommendations below are organized by jurisdiction and, within each, by three dimensions common to every framework reviewed in Sections 3 and 4: the Q-Day timeline itself, the quantum threat that timeline creates, and the quantum opportunity that the same underlying technology opens.

5.1 United States

On timeline, the United States should codify the Department of War's 2030 deadline for high-impact systems and 2031 deadline for force-wide migration as the default federal standard rather than a ceiling, while maintaining a standing, regularly updated public estimate of Q-Day timing — anchored to MITRE's 2035–2060 range — so that neither complacency nor overreaction shapes policy. On threat, federal agencies and critical-infrastructure operators should complete cryptographic inventories to close the harvest-now, decrypt-later exposure window, and NIST's post-quantum cryptography standards should be extended as an adoption requirement to federal contractors and critical-infrastructure sectors such as energy, finance, and healthcare, not federal agencies alone. On opportunity, coalition-based migration models such as the PQC Coalition can lower the cost of migration for small and mid-size critical-infrastructure operators, and a portion of the sixfold growth in quantum research and development investment documented by McKinsey should be directed toward dual-use quantum sensing and positioning, navigation, and timing capabilities, which are fielding faster than quantum computing itself.

5.2 United Kingdom

On timeline, the United Kingdom should hold firm to the National Cyber Security Centre's 2028, 2031, and 2035 milestone structure as the definitional national schedule, and regulated sectors such as financial services and energy should be required to publish milestone-linked migration status, building on the Financial Conduct Authority's early post-quantum guidance. On threat, the NCSC's Assured Cyber Security Consultancy pilot for post-quantum cryptography should be resourced to scale beyond pilot status into a standing national migration-support service, and university-industry security pipelines — Oxford's relationship with PQShield, Cambridge's Centre for Quantum Information and Foundations — should be given formal advisory roles in setting migration standards. On opportunity, the United Kingdom's academic strength in quantum key distribution and quantum sensing, embodied by firms such as KETS Quantum Security, Quantum Dice, and Riverlane, should be treated as an export and alliance-building asset with the United States and NATO, and the new Cambridge-IonQ Quantum Innovation Centre should serve as a template for further university-industry co-investment in quantum-security research.

5.3 NATO

On timeline, the Alliance should complete its own transition to quantum-safe cryptography — explicitly listed as a desired outcome of NATO's 2024 Quantum Technologies Strategy — and stand up the Transatlantic Quantum Community called for in that Strategy as the forum for harmonizing member-state Q-Day timelines. On threat, post-quantum cryptography and quantum key distribution support should be extended through NATO committees to reduce the risk that uneven member-state readiness becomes an Alliance-wide vulnerability, and Allies should monitor and voluntarily screen adversarial investment and interference in Allied quantum-technology supply chains, as the Strategy itself recommends. On opportunity, the Defence Innovation Accelerator for the North Atlantic and the NATO Innovation Fund should channel deep-tech investment toward dual-use quantum sensing, positioning, navigation, and timing, and secure communications across Allied militaries, and quantum technology integration should be formalized into defense-planning and capability-development cycles through the “learn-by-doing” approach the Strategy directs.

6. Summary of Findings

Four findings emerge from the preceding sections. First, the quantum-security industry is real, growing, and increasingly well-capitalized — quantum-technology investment grew sixfold, from two billion to thirteen billion dollars, between 2024 and 2025 — but it remains a market of several dozen serious participants per country rather than hundreds, and claims of comprehensive “top 100” rankings should be treated with caution. Second, academic thought leadership on Q-Day is concentrated at a small number of institutions: Oxford and Cambridge in the United Kingdom, and MIT, Harvard, and Stanford in the United States, each of which has produced both foundational research and direct commercial spin-outs, from [PQShield](#) to [Quantinuum](#)'s Cambridge lineage to the new Cambridge-[IonQ](#) centre. Third, the five major

consultancies surveyed converge on the same core message despite differing client bases: quantum readiness is fundamentally a leadership and governance issue rather than a purely technical one, and the gap between stated awareness and actual deployment remains wide, at eighty-seven percent planning against seven percent deployed at scale. Fourth, the United States, the United Kingdom, and NATO all operate on structurally similar timelines — milestone-based post-quantum cryptography migration mandates landing between 2028 and 2035 — which together create a genuine opportunity for allied standardization rather than fragmented, unilateral approaches.

7. Key Recommendations Overall

Across all three jurisdictions, five recommendations apply without modification. Cryptographic inventory should be treated as the universal first step, since no migration plan is credible without first knowing what needs to migrate. The three allied timelines — the U.S. schedule of 2030 and 2031, the UK's 2028, 2031, and 2035 milestones, and NATO's own transition — should be explicitly aligned rather than left to proceed independently, which risks creating interoperability gaps between allied systems precisely when interoperability matters most. Investment in quantum sensing and timing should proceed alongside investment in cryptography, since sensing and timing are fielding faster than quantum computing itself and deliver near-term resilience value, such as GPS-independent navigation, regardless of exactly when Q-Day arrives. Coalition and consortium models — the PQC Coalition, NATO's proposed Transatlantic Quantum Community, university-industry centers such as Cambridge-IonQ — should be used to spread migration cost and expertise rather than treating the transition as a purely national or purely corporate undertaking. Finally, quantum risk should be elevated to board and ministerial level, following the shared framing offered independently by KPMG and McKinsey: this is a governance and disclosure matter, not solely a technical project for chief information security officers to manage on their own.

8. Conclusion

Q-Day is best understood not as a single future event but as a slow-moving deadline that is already reshaping procurement, standards, and investment well before its arrival. The industry response documented in this paper is real but still maturing, concentrated in a few dozen credible companies per country rather than hundreds, and it is being outpaced by the scale of the migration task that lies ahead of it. The academic and consulting response is considerably more mature: five universities and five global consultancies, working independently and for different audiences, have each converged on the same conclusion — that quantum readiness is a leadership priority requiring action years ahead of any certainty about exactly when a cryptographically relevant quantum computer will exist. The United States, the United Kingdom, and NATO each already have credible, milestone-based plans in motion. The remaining work is less a matter of inventing new frameworks than of resourcing, aligning, and accelerating the

ones that have already been published, before the gap between planning and deployment becomes the vulnerability itself.

2026–28	2028–31	2031–35	2035+
Standards mature, crypto-agility spreads	High-impact systems migrate (US/UK)	Force-wide & national migration deadlines	Quantum-secured baseline expected

Figure 1. A decade of converging deadlines, from standards maturity to a quantum-secured baseline.

References

Bain & Company. (2026). Bain & Company announces strategic collaboration with IBM to deliver post-quantum cryptography assessment to private equity and corporate clients.

Booz Allen Hamilton. (2025). Booz Allen Ventures invests in quantum hardware innovation for national security.

Booz Allen Hamilton. (2025). Booz Allen and SEEQC expand partnership to accelerate quantum engineering solutions.

Centre for International Governance Innovation. (2024). “Q Day” is coming: Is the world prepared?

DigiCert. (2026). Quantum Readiness Outlook 2026.

Harvard Quantum Initiative. Harvard Gazette, various articles, news.harvard.edu.

IonQ. (2026). IonQ and University of Cambridge announce landmark agreement to establish Quantum Innovation Centre.

KPMG. (2026). Prepare now for quantum cyber risk. KPMG US Board Leadership.

KPMG. Quantum readiness. KPMG UK Insights.

McKinsey & Company. Quantum cybersecurity: Preparing for Q-Day and PQC.

MIT Quantum Initiative (QMIT). quantum.mit.edu.

NATO. (2024). Summary of NATO's Quantum Technologies Strategy.

PQShield. (2025). PQShield hits 100 research papers — pushing post-quantum cryptography from theory to reality.

Stanford University. (2019). Q-FARM initiative to bolster quantum research at Stanford-SLAC.

Tracxn. (2026). Top companies in quantum resistant cybersecurity / quantum computing in cybersecurity.

The Quantum Insider. (2026). 25 companies building the quantum cryptography and communications markets.

The Stack. (2025). PQShield raises £37m in Series B funding round.

QuantumZeitgeist. (2026). UK quantum computing companies 2026 directory; 15 UK quantum companies making waves in 2026.

Appendix: Adversary Naming Conventions

CrowdStrike adversary naming taxonomy

Cybersecurity vendors label state-linked and criminal threat actors using their own naming conventions to avoid confirming classified attribution while still communicating a group's likely origin. The table below reproduces one widely referenced taxonomy — CrowdStrike's animal-based adversary naming convention — for reference. This footnote is included for reader orientation only; it is not a finding of this paper and reflects a single vendor's classification system, which other vendors label differently.

Adversary Term	Attribution
Bear	Russia
Panda	People's Republic of China
Chollima	DPRK (North Korea)
Crane	ROK (Republic of Korea)
Kitten	Iran
Spider	eCrime
Jackal	Hacktivist
Tiger	India
Wolf	Türkiye
Leopard	Pakistan
Lynx	Georgia
Bison	Belarus
Ocelot	Colombia
Buffalo	Vietnam
Saiga	Kazakhstan
Sphinx	Egypt
Hawk	Syria

Part II

The Quanta Program: A Roadmap for Allied Quantum Readiness

Editorial note: the sections that follow are a forward-looking program roadmap prepared by Manage Defense International / Quanta Diplomacy. Where they reference existing government programs and policy (e.g., Golden Dome, White House and NATO quantum strategy), those references are factual and sourced. Programs bearing the “Quanta” name — Quanta Dome, Quanta Qube, Quanta Diplomacy Foundation, Quanta Universal, Quanta R&D, Quanta Future — are proposed concepts put forward in this roadmap, not existing government or fielded programs, and are illustrated accordingly as conceptual exhibits.

9.1 Q-Day USA/UK: Threats and Opportunities

For the United States and United Kingdom specifically, Q-Day is best framed as a shared clock running against two overlapping timelines: the Department of War's 2030/2031 migration gates and the UK National Cyber Security Centre's 2028/2031/2035 milestones (Sections 1 and 5). The threats and opportunities that follow from that clock are summarized below.

THREATS

- Harvest-now, decrypt-later collection against US/UK data
- Uneven agency & sector migration timelines
- Allied interoperability gaps if US/UK/NATO desync
- Legacy PKI embedded across critical infrastructure

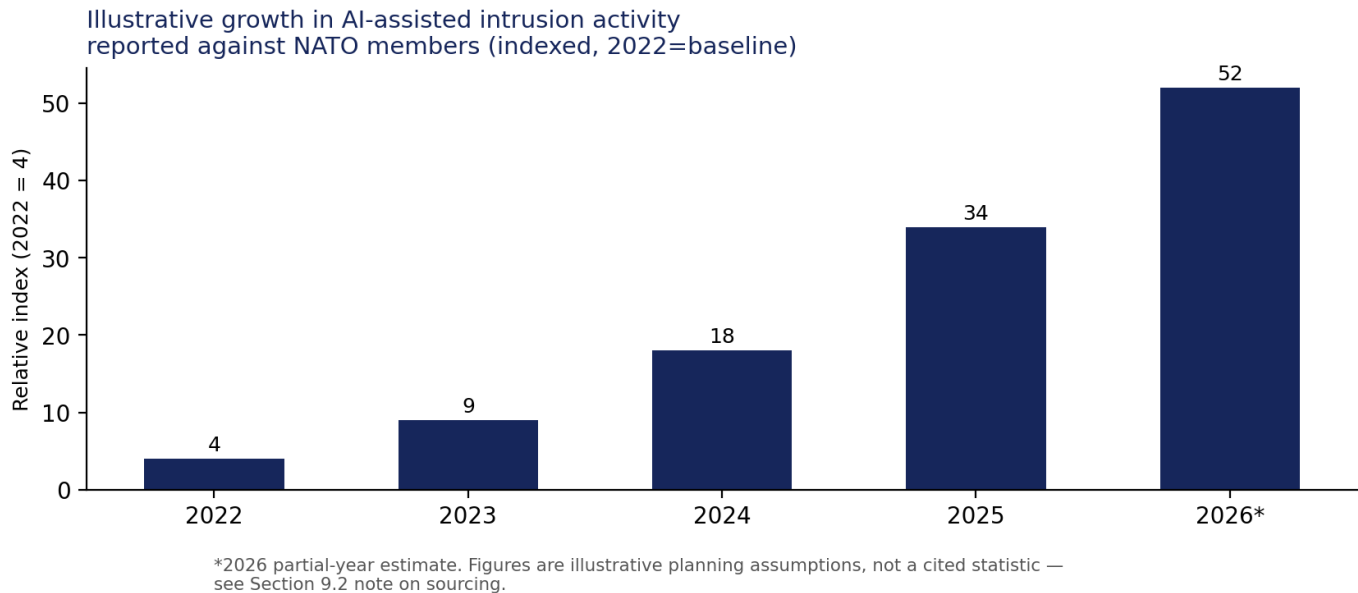
OPPORTUNITIES

- First-mover standard-setting via NIST + NCSC leadership
- Export strength in QKD & quantum sensing (UK)
- Dual-use PNT and sensing fielding ahead of computing
- Alliance-wide crypto-agility as a shared capability

The throughline for both countries is the same one identified in Section 6: the gap between planning (eighty-seven percent of organizations, per DigiCert) and deployment at scale (seven percent) is itself the central vulnerability. Preparing for Q-Day in the US/UK context means closing that gap on a shared schedule rather than two separate national ones, so that allied systems remain interoperable as each country migrates.

9.2 AI Malware Across NATO: Statistics and Actors

AI-assisted malware — malicious code that uses machine-learning components for obfuscation, target selection, or autonomous decision-making during an intrusion — is a fast-moving and inconsistently measured category. No single, authoritative, publicly available count of AI-assisted intrusions against NATO members currently exists, in the same way that no verifiable “top 100” ranking of quantum-security companies exists (Section 2). The chart below is an illustrative planning curve, not a cited statistic, and should be treated as a placeholder for the Alliance's own classified and open-source reporting rather than as a sourced figure.



The state-linked and criminal actors most frequently associated with AI-enabled intrusion activity against NATO members follow the same naming conventions summarized in the Appendix: Russian GRU, FSB, and SVR units; Chinese state-linked “Panda” groups; DPRK “Chollima” groups; and Iranian “Kitten” groups. A dedicated, sourced assessment of AI-malware activity by actor would need to draw on classified NATO reporting and named-vendor threat intelligence rather than the open literature surveyed in this paper, and is recommended as a companion product to this roadmap rather than an extension of it.

9.3 National Security Imperative

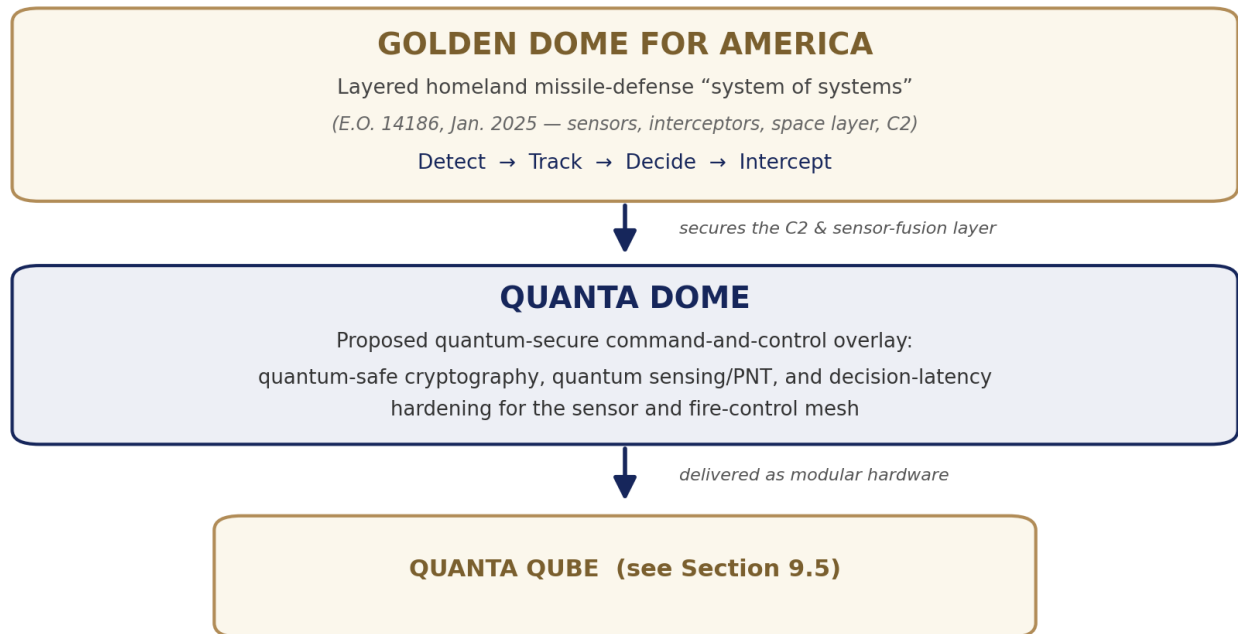
The case for treating quantum readiness as a national security imperative, not an IT project, is now made directly in primary policy documents from all three branches of the U.S. government, alongside NATO's own strategy:

- **White House** — National Security Memorandum 10 (May 2022) directed agencies to begin migration planning; two June 22, 2026 executive orders, “Securing the Nation Against Advanced Cryptographic Attacks” and “Ushering in the Next Frontier of Quantum Innovation,” converted that planning into enforceable federal deadlines (Dec. 31, 2030 for key establishment; Dec. 31, 2031 for digital signatures) and created the QC-ADDS effort at the Department of Energy.
- **Pentagon (Department of War)** — has set its own 2030/2031 high-impact and force-wide migration gates (Section 1), and is separately leading the Golden Dome for America missile-defense program under Executive Order 14186, discussed in Section 9.4.
- **Congress / Senate** — the Post Quantum Cybersecurity Standards Act (H.R. 3259, 119th Congress) would codify NIST's role in promoting post-quantum cryptography adoption government-wide, alongside FY2025 reconciliation funding that provided the initial \$24.4 billion tranche for Golden Dome.
- **NATO** — the 2024 Quantum Technologies Strategy (Section 5.3) sets Alliance-wide expectations that mirror the U.S. and UK timelines.

9.4 Quanta Dome

Golden Dome for America is the real, currently funded homeland missile-defense initiative directed by Executive Order 14186 (January 27, 2025): a layered “system of systems” combining space-based sensors, interceptors, and command-and-control, with an initial \$24.4 billion appropriated through the FY2025 reconciliation law and procurement running through the Missile Defense Agency’s SHIELD contract vehicle.

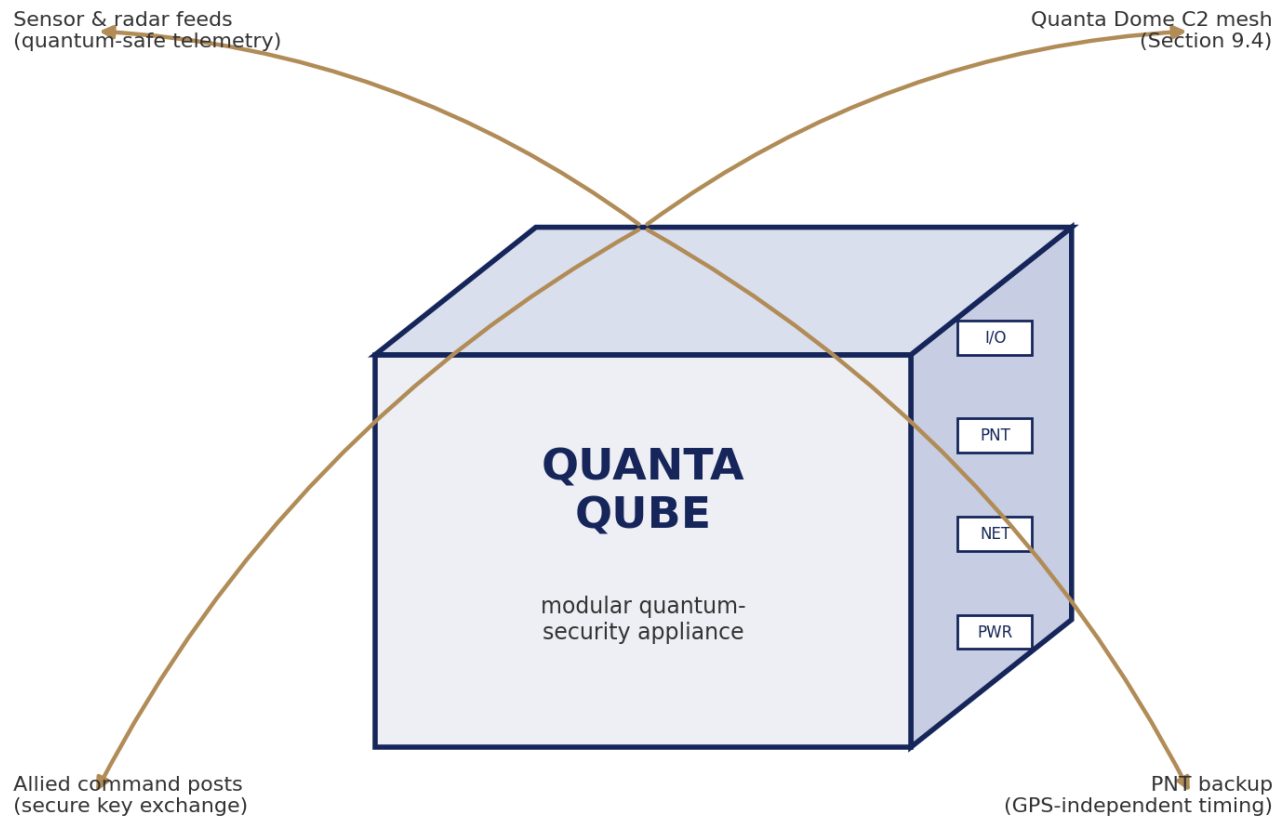
Quanta Dome, proposed here, is not a Golden Dome program element — it is a concept for how a quantum-secure overlay could harden the sensor-fusion and command-and-control layer that any system of Golden Dome’s scale will depend on: quantum-safe cryptography for the data links between sensors and interceptors, and quantum sensing/PNT as a GPS-independent backup for the timing that layered missile defense requires.



Conceptual illustration — Quanta Dome/Qube are proposed Quanta Diplomacy programs, not an official DoD or Golden Dome program element.

9.5 Quanta Qube

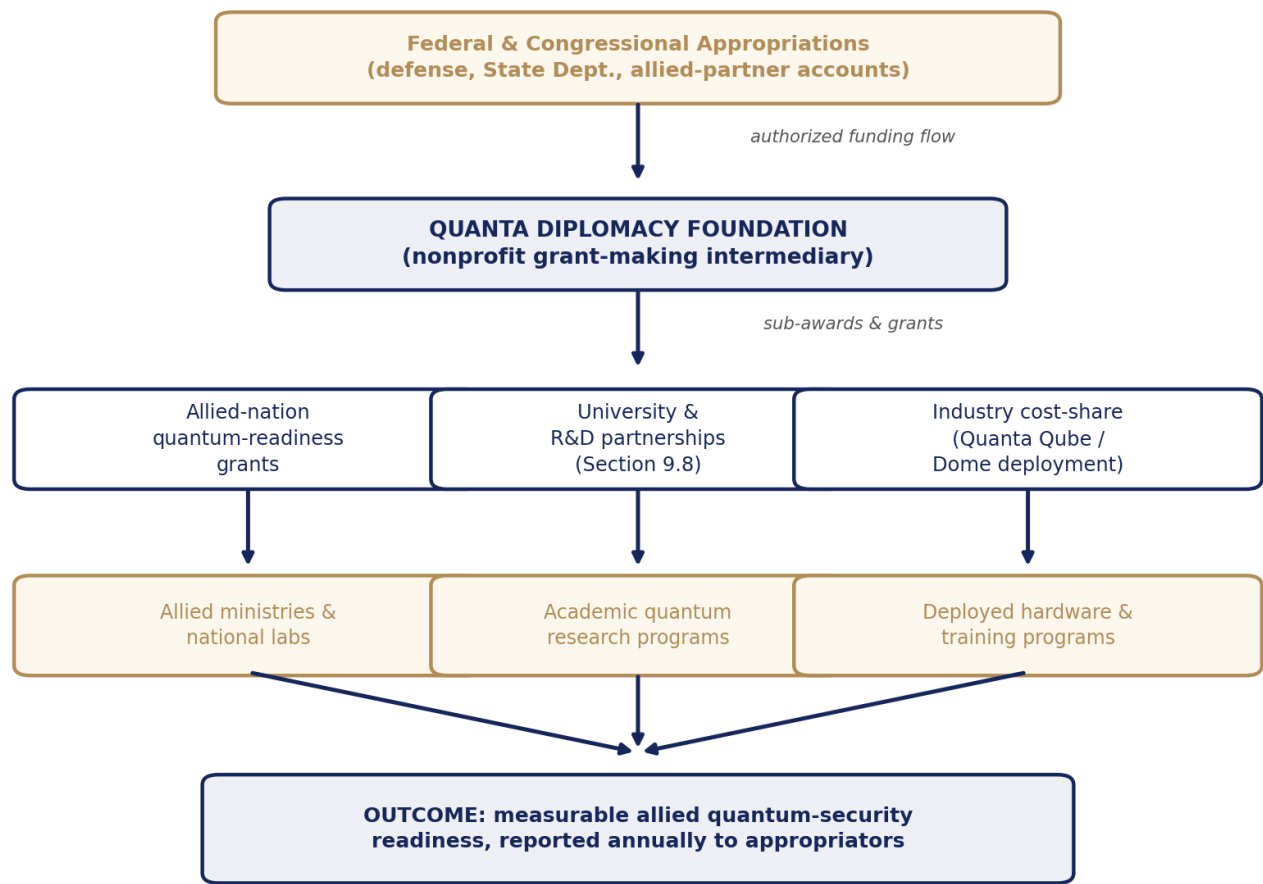
Quanta Qube is the proposed hardware form factor for delivering Quanta Dome's capability: a modular, field-deployable appliance rather than a data-center-scale installation, designed to sit between existing sensor/radar feeds and a command post's network, presenting quantum-safe key exchange and PNT backup through standard power, network, timing, and I/O interfaces.



Conceptual illustration — Quanta Qube is a proposed hardware concept, not a fielded product.

9.6 Quanta Diplomacy Foundation

The Quanta Diplomacy Foundation is proposed as a nonprofit grant-making intermediary that would sit between congressional/federal appropriations and the allied ministries, universities, and industry partners who actually deploy quantum-readiness capability — modeled loosely on how coalition mechanisms such as the PQC Coalition already spread migration cost across smaller organizations (Section 7). The flow below illustrates how appropriated funding could move from Congress through the Foundation to three downstream tracks and, ultimately, to reportable readiness outcomes.



Conceptual illustration — Quanta Diplomacy Foundation is a proposed grant-making structure; actual appropriations authority rests with Congress.

9.7 Quanta Universal

Quanta Universal is proposed as a public-education initiative — a “PBS of quantum” — aimed at the same awareness gap identified throughout this paper: general audiences, and even many technology and policy professionals, do not yet have an accessible entry point into what Q-Day means or why the organizations profiled in Sections 3 and 4 are racing to prepare for it. A ten-year conceptual programming lineup is illustrated below, moving from general explainer content toward applied, then consumer-facing, programming as the underlying technology matures.

QUANTA UNIVERSAL — A DECADE OF PROGRAMMING

conceptual public-broadcasting-style lineup for quantum literacy



Conceptual illustration — Quanta Universal is a proposed public-education initiative, not an existing broadcast network.

9.8 Quanta R&D

To make the scale of quantum-computer acquisition concrete, the table below walks through an illustrative, standard-operating-line-item breakdown of what an approximately \$111 million utility-scale quantum-computer acquisition might include — covering not just the qubit hardware itself but the cryogenic infrastructure, control electronics, software stack, facility build-out, security accreditation, and sustainment that a real acquisition of this scale requires. These figures are illustrative planning assumptions, not drawn from a specific vendor quote or contract.

QUANTA R&D — ILLUSTRATIVE STANDARD OPERATING LINE ITEMS

Example cost breakdown for an approximately \$111M utility-scale quantum-computer acquisition

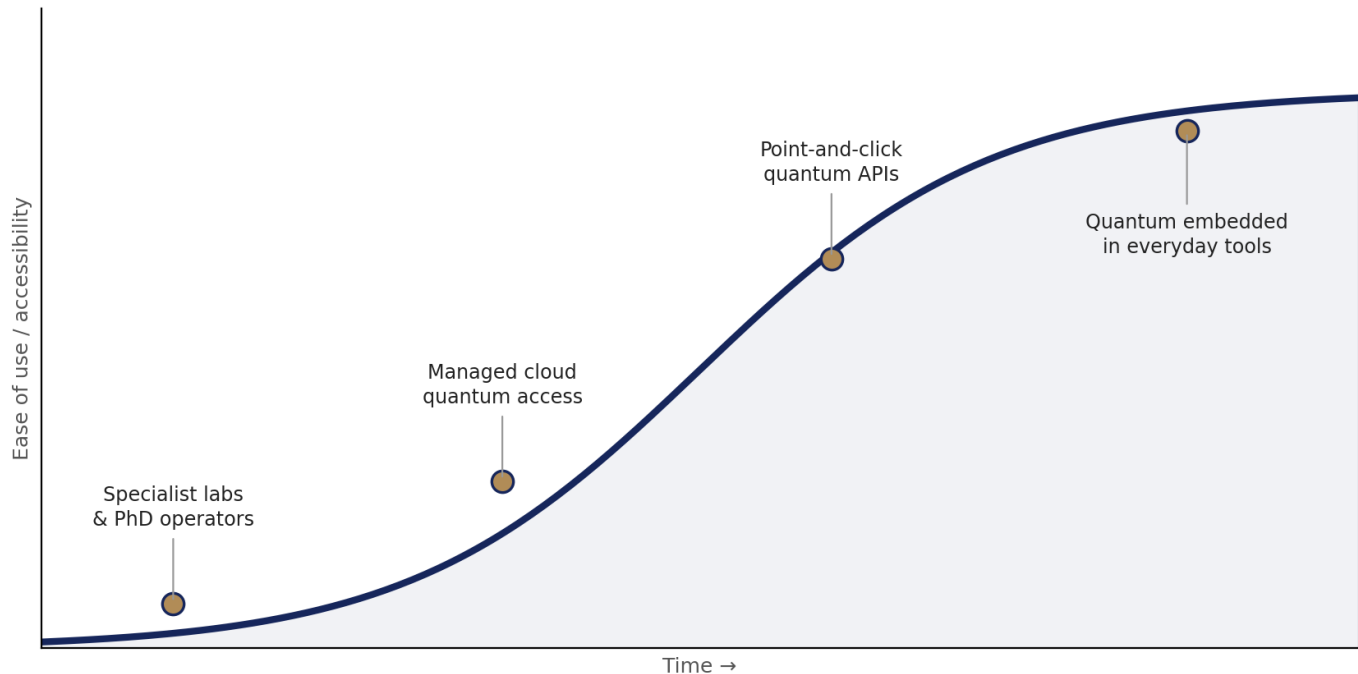
Standard Operating Line Item	Illustrative Cost
Superconducting / photonic qubit fabric & cryostat integration	\$38,500,000
Cryogenic infrastructure (dilution refrigeration, shielding)	\$14,200,000
Control electronics & signal chain (RF/microwave, FPGA)	\$11,800,000
Quantum error-correction & compiler software stack	\$9,600,000
Facility build-out & vibration/EMI isolation	\$8,900,000
Systems integration, install & commissioning	\$7,400,000
Workforce training & operator certification	\$4,100,000
Security accreditation (facility, personnel, TEMPEST)	\$5,300,000
Sustainment & extended warranty (Year 1)	\$6,200,000
Program management & contingency reserve (~4.5%)	\$5,000,000
TOTAL (illustrative)	\$111,000,000

Illustrative example only — actual quantum-computer procurement costs vary widely by modality, vendor, and contract vehicle; figures are not drawn from a specific program.

9.9 Quanta Future

The long-run trajectory implied by Sections 2 through 4 is one of steadily simplifying access: today's quantum computing still largely requires specialist operators and dedicated facilities, but the same pattern seen in classical computing — mainframe, to cloud, to API, to embedded utility — is already visible in early managed-quantum-cloud offerings from firms such as IBM and Quantinuum (Sections 2 and 3). Quanta Future frames this as a simplification curve: the point of the programs proposed in this roadmap is to compress that curve for allied governments rather than wait for the commercial market to do it unassisted.

QUANTA FUTURE — SIMPLIFYING ACCESS TO QUANTUM COMPUTING



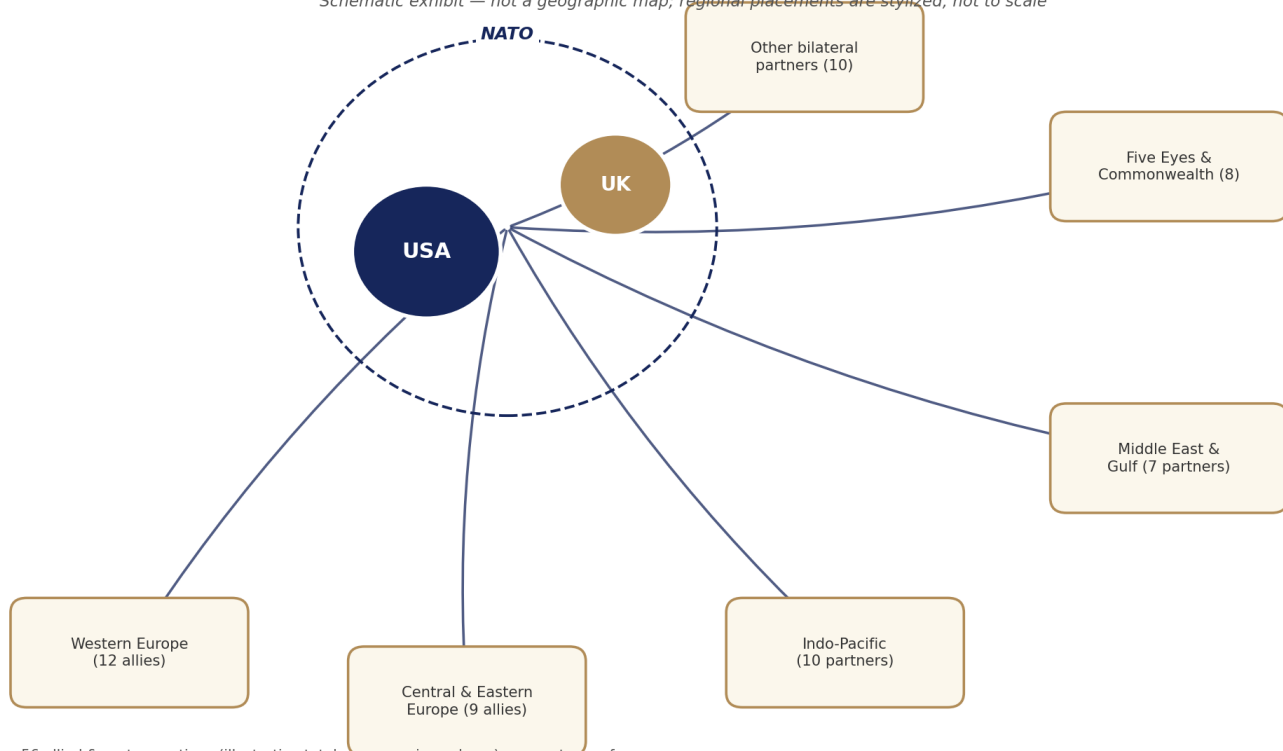
Conceptual illustration — an adoption curve, not a forecast tied to a specific vendor or date.

Exhibit: US/UK Quantum Technology Supply to Allied Nations

The exhibit below illustrates, schematically, how a Quanta Dome/Qube-style capability could extend from the United States and United Kingdom to a broader base of allied and partner nations across six regions, alongside NATO's own Quantum Technologies Strategy (Section 5.3). This is a conceptual planning exhibit prepared for this roadmap, not a geographic map or an official tally of current agreements.

ILLUSTRATIVE SUPPLY NETWORK: US & UK QUANTUM TECHNOLOGY TO ALLIED NATIONS

Schematic exhibit — not a geographic map; regional placements are stylized, not to scale



56 allied & partner nations (illustrative total across regions above) — quantum-safe communications, sensing/PNT, and QKD infrastructure, delivered alongside NATO's own quantum-technology strategy. Figures are a conceptual planning exhibit, not an official count.