Quantum for National Security: Roadmaps, Policy, Partnerships, and Acquisitions (DRAFT)

Paul F. Roysdon, Ph.D.

November 15, 2025

Abstract

Quantum computing is crossing from physics demonstration to a decade-scale engineering program with profound national-security implications. Credible resource estimates place the threshold for breaking RSA–2048 at roughly one million physical qubits with days-to-weeks runtime, while thousands of logical qubits can unlock transformative simulation in chemistry, materials, and optimization. The challenge has shifted to systems engineering: cryogenics, power, interconnects, decoding, facilities, and workforce. This paper proposes a national roadmap to 2035; a federal implementation plan; policy, governance, and standards actions; partnership constructs; and rapid acquisition pathways tailored to quantum hardware, decoders, and mega-scale facilities.

1 Strategic Imperative and Current Posture

Quantum advantage at scale has become a race in engineering rather than basic physics. Leading U.S. and allied firms—IBM, Google, Microsoft, Intel, Quantinuum, IonQ, PsiQuantum, and others—pursue diverse hardware paths (superconducting, trapped-ion, neutral-atom, photonic, silicon spin, and topological). Federal programs (NQI, DARPA US2QC, IARPA LogiQ/ELQ, DOE QIS Centers) target logical-qubit demonstrations, million-qubit architectures, and quantum networking. Execution will require multi-billion-dollar investments, specialized facilities in the 10–100 MW class, and a workforce spanning physics, cryogenics, photonics, RF/microwave, ASIC, controls, and cybersecurity.

2 State of the Art: Hardware, Theory, and Systems

2.1 Hardware platforms

Superconducting transmons offer fast gates and steady fidelity gains, with chips beyond a thousand qubits and super-fridges demonstrating scale. Trapped ions provide highest fidelities and all-to-all connectivity in small registers with modular photonic interconnects. Neutral atoms yield large, reconfigurable arrays with improving two-qubit fidelities. Photonic cluster-state approaches favor manufacturability and room-temperature operation. Silicon spin qubits promise CMOS density, long coherence, and cryo-CMOS control co-integration.

2.2 Error correction and algorithms

Surface-code experiments have entered the error-suppressing regime, with logical error rates decreasing as code distance increases. Advances in magic-state factories, lattice surgery, and tailored decoders reduce overheads for non-Clifford resources. Updated resource estimates place RSA–2048 within reach at roughly one million physical qubits and week-scale runtimes under realistic assumptions. Chemistry and materials targets appear feasible with 10^2–10^3 logical qubits.

2.3 Systems constraints

The dominant challenges are off-chip: (i) cryogenics and power (super-fridges or farms of dilution refrigerators), (ii) high-throughput decoding (on the order of 10^9 syndrome measurements/s), (iii) ultra-low-latency interconnects and cryo-proximate processing, and (iv) secure, vibration-managed facilities co-sited with classical HPC clusters.

3 Threat Landscape and Opportunity

- **Cryptography risk:** PQC migration and crypto-agility must accelerate; archival data faces "harvest-now, decrypt-later" risk.
- **Strategic science:** Quantum simulations can accelerate catalysts, batteries, fertilizers, and pharmaceuticals.
- **Optimization/logistics:** Hybrid quantum-classical solvers promise gains ahead of full fault tolerance.
- **Deterrence and assurance:** Demonstrated U.S. capability in logical-qubit performance, decoding, and secure networking sets norms and deters coercion.

4 National Quantum Roadmap (2025–2035)

4.1 Phase I—Secure & Prepare (2025–2026)

Mandate PQC migration plans, complete crypto inventories, and fund toolchains and independent testing labs. Launch a decoder-ASIC program targeting cryo-proximate operation and $> 10^9$ syndrome/s per rack. Prioritize grid interconnection and on-site generation for quantum/HPC campuses designated as critical energy loads.

4.2 Phase II—Prototype & Network (2027–2029)

Demonstrate 10–50 logical qubits with sustained error suppression; stand up 1k–10k physical-qubit modules networked via photonics; break ground on 50–150 MW Tier-1 campuses; pilot a National Quantum Interconnect (NQI-Net) with metro-scale entanglement links.

4.3 Phase III—Scale & Field (2030–2032)

Reach 100–300 logical qubits with first fault-tolerant application wins in chemistry/materials; deploy dedicated low-latency decoder datacenters; complete PQC deployment across federal systems and implement export controls on sensitive decoders and cryo subsystems.

4.4 Phase IV—Million-Qubit Era (2033–2035)

Integrate $\geq 10^6$ physical qubits across modular cryostats; achieve days-to-weeks execution of top-end algorithms; ensure allied interoperability and sovereign control of decoders, cryogenics, and toolchains.

Table 1: Milestones and Metrics

Year	Target	Example Metric	Outcome
2026	PQC pilots	$> 95\%$ crypto inventory	Gateways in prod.
2027	10 logical qubits	$< 10^{-6}$ per cycle	Stable suppression
2028	50 logical qubits	< 1 kcal/mol chemistry	$> 80\%$ uptime
2029	Networked modules	Inter-module entanglement	Photonic links
2031	100–300 logical	$> 10^9$ syndromes/s	FT app wins
2033+	$\geq 10^6$ physical	Days–weeks runtime	Sovereign capability

5 Federal Roadmap

5.1 Elements of power

White House Office of Science and Technology CTO establishes a *Quantum White Board* to prioritize IC & DoW (formerly DoD) use cases (crypto risk, strategic materials, SIGINT pipelines, geospatial simulation). Establish a National Quantum Council (NQC) chaired by the White House with NSC, NEC, OSTP, OMB, DOE, DoD, DHS, Commerce/NIST, and NSA to set binding policies for algorithm testing, PQC schedules, key management, and data sharing. Create a Quantum Academy with rotational billets at frontier vendors.

5.2 Infrastructure tiers

- **Tier-1 Campus (Fort Meade region):** 200 MW co-location of cryo halls and decoder/HPC clusters for classified research.
- **Tier-2 Pods:** 10–20 PF decode/inference capacity near mission hubs.
- **Tier-3 Kits:** ruggedized PQC gateways, time-transfer, and quantum-network taps for forward sites. A zero-trust data fabric with S3-compatible archives, WORM tiers, and confidential computing underpins all tiers.

6 Policy and Governance

The NQC should then direct NIST to publish Quantum Risk Profiles and Decoder Latency Standards. Designate quantum campuses as Critical Infrastructure; implement narrowly scoped export controls on high-performance decoders, cryogenic amplifiers, and photonic source arrays. Expand workforce pipelines and fund 20+ university Quantum Foundry Centers.

7 Partnerships

7.1 Prime facility contractors

Jacobs and Parsons are strong candidates to prime mega-scale, secure quantum/HPC campuses, with experience delivering 100+MW facilities, advanced cryogenics, and IC/DoD-grade security programs similar to their existing mega-scale data center projects for AI.

7.2 Industry, labs, universities

Semiconductor partners: GlobalFoundries, Intel, and IMEC for spin and photonic integration, including cryo-CMOS. System vendors: IBM, Google, Microsoft (Majorana), Intel (spin), Quantinuum and IonQ (ions), PsiQuantum and Xanadu (photonics), Rigetti (superconducting), Alice&Bob (cat codes). DOE centers (SQMS, Q-NEXT, QSA), NIST metrology and PQC, and NSF Quantum Leap institutes anchor the research base; Yale, UMD/Duke, Delft/QuTech, UChicago, Harvard, Stanford lead on theory and devices.

8 Acquisitions: Rapid, Modular, Accountable

8.1 Quantum Rapid Fielding Pathway (QPRA)

Create a FAR subpart modeled on OTA flexibility for 18–24 month rapid fielding, with milestone-based down-selects: breadboard → engineering prototype → limited operations → production. Stand up pre-negotiated consortia with cleared partners across hardware, decoders, cryogenics, facilities, and PQC.

8.2 Contracting patterns

Use modular CLINs: (i) cryo plant, (ii) qubit modules, (iii) decoders/ASICs, (iv) photonic interconnects, (v) facilities. Tie incentives to logical error rate, decoder latency, uptime, and algorithm completion metrics (e.g., chemical accuracy). Streamline data access with standardized SBU/Q-SBU enclaves and red-team validation.

8.3 Security and compliance

Adopt zero-trust from day one; confidential computing for decoder clusters; SBOMs for firmware; continuous monitoring. Assure supply chains with on-shore fabrication for sensitive ASICs, tamper-evident packaging, and hardware attestation.

9 Facility Blueprint and Energy Strategy

Cryogenic architecture may comprise hundreds of dilution refrigerators or multi-bay super-fridges (e.g., Goldeneye-class) delivering 10 mW at 100 mK and > 20 W at 4 K per unit; centralized helium plant; vibration isolation and EMI shielding. Plan for $10 - 50$ MW initial power, expandable to ≥ 100 MW, with dual utility feeds, on-site gas turbines with heat reuse, and potential SMR integration. Facilities require multi-thousand m^2 labs and cleanrooms, laser halls, and secure HPC/decoder rooms. Workforce scales to several hundred across disciplines, with automation for calibration.

10 Risk Register and Mitigations

- **Decoder bottlenecks:** Invest in ASICs, hierarchical decoding, and cryo-proximate processing; set latency budgets and test them.
- **Cryogenic scale-out:** Diversify platforms to reduce mK load; pursue super-fridge and modular designs; maintain spare capacity.
- **Supply chain:** On-shore fabrication for detectors, amplifiers, and ASICs; multi-vendor sourcing and strategic reserves for helium/cryogens.
- **Talent scarcity:** IC Quantum Academy, scholarships, allied exchanges, and prioritized visas for quantum specialists.
- **PQC deployment lag:** Mandated deadlines, crypto-agility tooling, and red-team exercises; protect sensitive archives against harvest-now/decrypt-later.

11 Conclusion

The path to a million-qubit, fault-tolerant quantum computer is sufficiently clear to plan, finance, and execute. Success now depends on disciplined systems engineering, decisive policy, and rapid yet secure acquisition. By coupling PQC urgency with an aggressive build-out of sovereign quantum capability, the United States can deter adversaries, accelerate discovery, and secure long-term technological leadership.

Acknowledgments

The author thanks colleagues across industry and academia for discussions and publications that informed this work.

Note on References

While there are many research papers that span these topics, this article emphasized papers with the following metrics:

- ✓ High Citation Counts – Many references have 1,000+ citations, ensuring they are widely accepted and influential in the Quantum, Math, Policy, Economics, and National Security research community.
- ✓ Top Quantum, Math, Policy, Economics, and National Security Institutions – Includes research from Stanford, CSET, GWU, and Harvard.
- ✓ Authors with High h-Index – leading AI researchers such as Craig Gidney (h-index: 150+).

References

[1] "IBM aims for quantum computer in 2029, lays out road map for larger systems," Reuters. https://www.reuters.com/business/retail-consumer/ibm-aims-quantum-computer-2029-lays-out-road-map-larger-systems-2025-06-10/

[2] "Trump signs legislation to boost quantum computing research with $1.2 billion," GeekWire https://www.geekwire.com/2018/trump-signs-legislation-back-quantum-computing-research-1-2-billion/

[3] Quantum Computing: Whose Qubit is Better? @ ISSCC 2025 https://sscs.ieee.org/event/quantum-computing-whose-qubit-is-better/

[4] Hanhee Paik (IBM) - IBM's 1000-qubit Condor and QEC plans, coherence and fidelity metrics

[5] Shirin Montazeri (Google) - Scaling control electronics to millions of qubits, challenge and opportunity

[6] Sophie Bene (imec) - Silicon spin qubits: long coherence and CMOS scalability

[7] Jeanette Roberts (Intel) - Spin qubits for fault-tolerance, millions of qubits with fab tech

[8] Eleventh Hour Enthusiast (Medium) - Trapped-ion hardware and performance, overview of ion trap advantages (identical qubits, high fidelity, all-to-all connectivity) https://medium.com/@EleventhHourEnthusiast/ion-based-quantum-computing-hardware-performance-and-end-user-perspective-d1b7ab24de7c

[9] Eleventh Hour Enthusiast (Medium) - Neutral atom hardware and performance, Rydberg gates, coherence ∼ seconds, fidelities ∼99% https://medium.com/@EleventhHourEnthusiast/neutral-atom-quantum-computing-hardware-performance-and-end-user-perspective-98c13456ad23

[10] Quandela Glossary - Photonic qubits, encodings and challenges (single-photon sources, detectors, lack of native two-qubit interactions) https://www.quandela.com/resources/quantum-computing-glossary/photonic-qubit/

[11] Silicon spin qubit advances, 0.5 s coherence, 99.95% 1-qubit and 99% 2-qubit fidelity at 1 K https://phys.org/news/2025-05-silicon-qubits-gain-ground-candidate.html

[12] The Verge (Google AI) - Google's quantum roadmap, targeting 1,000,000 physical qubits by 2029 for error-corrected machine

[13] Reuters (IBM 2025) - IBM roadmap, practical quantum computer by 2029 (200 logical qubits) and larger (>200 logical) by 2033

[14] Google Security Blog (Gidney et al. 2025) - Resource estimate for breaking RSA-2048, reduced from 20M to 1M qubits via algorithm and QEC improvements

[15] Microsoft Azure Blog (2025) - Majorana qubits and roadmap, Majorana 1 chip designed to scale to a million qubits on one chip

[16] Interesting Engineering (PsiQuantum) - Planned Chicago quantum facility, goal of 1 million fault-tolerant qubits, partnering with government https://interestingengineering.com/innovation/psiquantum-quantum-computing-facility-us

[17] IBM Blog (2022) - Project Goldeneye super-fridge, 1.7 m^3 dilution refrigerator for large experiments, groundwork for scaling

[18] National Quantum Initiative Annual Report FY2024 - DARPA US2QC and other agency efforts, three companies contracted in 2023 to design utility-scale QC

[19] IEEE Spectrum / HPCwire - IBM's 127-qubit and 433-qubit achievements, quantum volume 128->256, plan for 1121-qubit Condor in 2023 https://www.ibm.com/quantum/blog/quantum-metric-layer-fidelity

[20] Spin Quanta - How Josephson Junctions Power Quantum Computing https://www.spinquanta.com/news-detail/the-role-of-josephson-junctions-in-quantum-computing

[21] PsiQuantum "A manufacturable platform for photonic quantum computing" https://www.nature.com/articles/s41586-025-08820-7

[22] "Linear Optics to Scalable Photonic Quantum Computing" https://arxiv.org/html/2501.02513v1

[23] "Alice & Bob to Build $50 Million Advanced Quantum Lab in Paris" https://alice-bob.com/newsroom/alice-bob-product-development-lab

[24] LogiQ (Logical Qubits) https://www.iarpa.gov/research-programs/logiq

[25] "IARPA Pursuing Significant Advancement in Quantum Computing" https://www.odni.gov/index.php/newsroom/press-releases/press-releases-2024/3772-iarpa-pursuing-significant-advancement-in-quantum-computing