European Economic Letters
ISSN 2323-5233
Vol 15, Issue 1 (2025)
http://eelet.org.uk

The Efficacy of Quantum Computing in E-Governance and the Public Sector: Statistical Models, Projections, and Predictive Analysis

Dr. Abhishek Roy
Chief Technology Officer, Government of West Bengal, India. drroyabhishek@gmail.com

Dr. Madhu Bala Roy
Associate Professor, Management Department, Techno India University, West Bengal India. email:- drmadhubalaroy@gmail.com

Abstract

Quantum computing (QC) promises to deliver computational advantages over clas- sical computing for certain classes of problems. In e-governance and public sector functions—such as cybersecurity, policy optimization, service delivery, and administrative decision support—these advantages may translate into improve- ments in efficiency, security, transparency, and scalability. This paper critically ex- amines the current literature, constructs statistical and predictive models, and estimates financial and operational projections to assess the likely impact (positive and negative) of deploying quantum computing in public sector governance over the next 10–20 years. We find that with moderate to aggressive adoption, the benefits, particularly security resilience and efficiency gains, substantially outweigh the costs within a medium-term horizon.

Keywords: quantum computing, e-governance, public sector, cybersecurity, pre- dictive modelling, projections, post-quantum cryptography, policy analysis.

1. Introduction: The Quantum Imperative in Digital Governance

E-governance refers broadly to government operations and service delivery mediated by digital systems. Key concerns include data security, transparency, cost, efficiency, cit- izen trust, and scalability. The advent of quantum computing introduces a duality: **unprecedented opportunities** (e.g., faster optimization, novel algorithms for predic- tion, enhanced simulation) and **severe, existential risks** (e.g., the potential to break foundational classical cryptographic algorithms like RSA and ECC) [1].

This paper addresses this duality by developing statistical models to project key public sector outcomes—specifically focusing on security incidents, service latency, cost, and cit- izen trust—across varied QC adoption scenarios. This structured, quantitative approach provides a reasoned storyline for policy recommendations.

2. Literature Review: Assessing the Threat and the Promise

2.1 The Cryptographic Threat and Post-Quantum Mitigation

The most immediate and critical concern for the public sector is the quantum threat to cybersecurity. **Shor's algorithm** poses a direct threat to widely used asymmetric cryptosystems, which form the bedrock of secure communication and digital signatures in e-governance [2]. This necessitates a time-critical, mandatory system upgrade.

Post-Quantum Cryptography (PQC) schemes, currently being standardized by bodies like NIST [3], are the primary mitigation pathway. Their adoption is crucial to safeguard citizen data, identity systems, and critical infrastructure.

2.2 Quantum Opportunities in Optimization and AI

QC offers computational speedups in complex optimization, simulation, and machine learning tasks:

- **Policy Optimization:** Quantum algorithms can solve NP-hard problems related to resource allocation, logistical planning (e.g., disaster relief), and budget opti- mization at greater speed [4].
- **Case Studies:** Initiatives like the **MeitY Quantum Computing Applications Lab (India)** [5] and industry consortia like **QUTAC (Europe/Germany)** [6] are prototyping solutions for resource planning and advanced forecasting.

2.3 Economic Projections

The economic impact is projected to be substantial, with the **Boston Consulting Group (BCG)** projecting QC could generate **US$ 450–850 billion** in global economic value by 2040 [7]. However, challenges remain, including hardware limitations (NISQ devices) and integration costs [8].

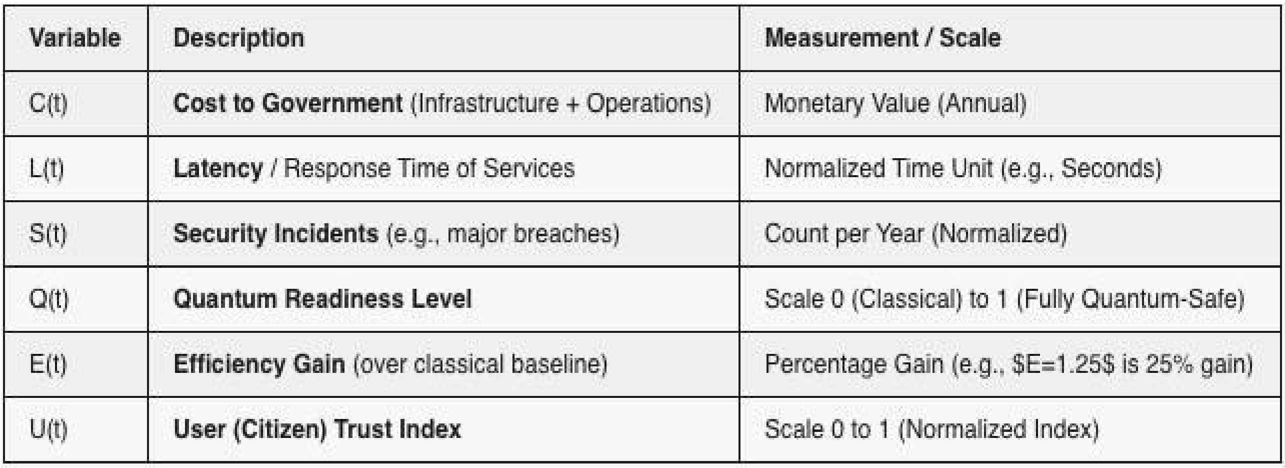
3. Theoretical Framework and Model Design

To assess efficacy, we construct models to measure outcomes under classical vs. quantum-enhanced systems.

3.1 Key Variables and Definitions

Key variables include:

- $C(t)$: Cost to government (infrastructure + operations).
- $L(t)$: Latency / response time of services.
- $S(t)$: Number of security incidents per year.



Variable	Description	Measurement / Scale
C(t)	**Cost to Government** (Infrastructure + Operations)	Monetary Value (Annual)
L(t)	**Latency** / Response Time of Services	Normalized Time Unit (e.g., Seconds)
S(t)	**Security Incidents** (e.g., major breaches)	Count per Year (Normalized)
Q(t)	**Quantum Readiness Level**	Scale 0 (Classical) to 1 (Fully Quantum-Safe)
E(t)	**Efficiency Gain** (over classical baseline)	Percentage Gain (e.g., $E=1.25$ is 25% gain)
U(t)	**User (Citizen) Trust Index**	Scale 0 to 1 (Normalized Index)

3.2 Base Models

3.2.1 Cost–Benefit Analysis (Net Present Value)

Initial investment I is amortized over N years. The net present value (NPV) over horizon T is defined as:

$$\text{NPV} = \sum_{t=1} \frac{B(t) - C_{\text{quantum}}(t)}{(1+r)^t}$$

Where $B(t)$ denotes aggregate monetary benefit, $C_{\text{quantum}}(t)$ includes initial investment and maintenance overheads $c_{\text{maint}}(t)$, and r is the discount rate. A positive NPV indicates a financially viable investment.

3.2.2 Predictive Model of Security Incidents (Mitigation)

The expected security incidents under quantum-resistant cryptography (S_q) are modeled as:

$$S_q(t) = S_0 \cdot e^{-\alpha Q(t)}$$

Where S_0 is baseline classically-attacked incidents, and α is the effectiveness parameter of QC/PQC in reducing incidents.

3.2.3 Service Latency and Efficiency Gains

Efficiency gain $E(t)$ is assumed to correlate linearly with readiness $Q(t)$:

$$E(t) = 1 + \beta Q(t)$$

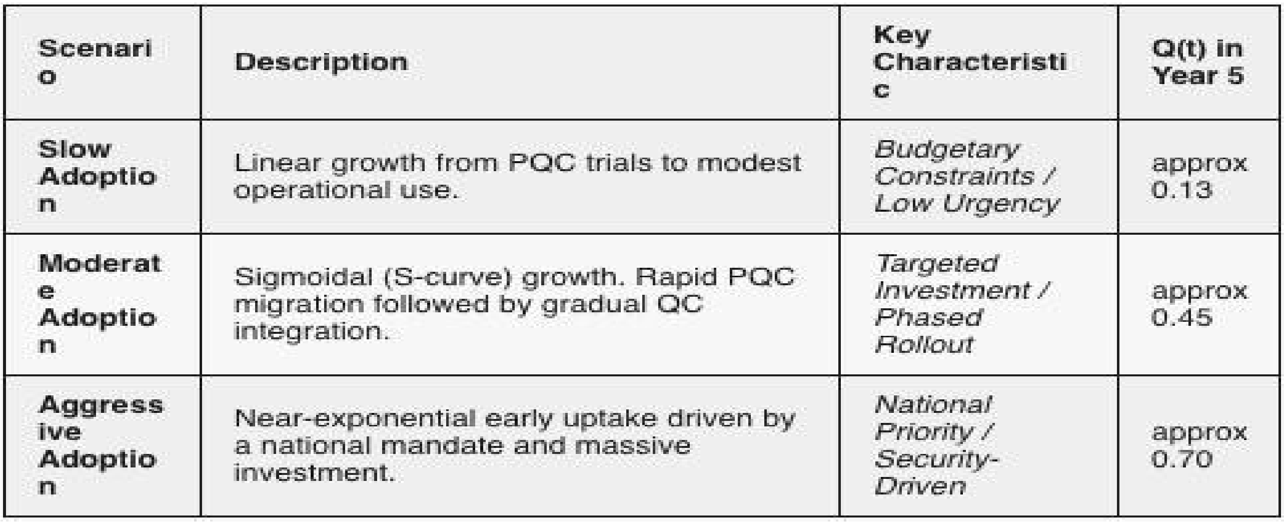
Where β quantifies the maximum achievable efficiency gain. Latency $L(t)$ is inversely correlated:

$$L(t) = L_0/E(t) + \delta$$

Where L_0 is the baseline latency and δ represents minimal non-computational delays.

3.3 Projection Scenarios for $Q(t)$

Three scenarios define the evolution of the Quantum Readiness Level over a 15-year horizon:



Scenario	Description	Key Characteristic	Q(t) in Year 5
Slow Adoption	Linear growth from PQC trials to modest operational use.	*Budgetary Constraints / Low Urgency*	approx 0.13
Moderate Adoption	Sigmoidal (S-curve) growth. Rapid PQC migration followed by gradual QC integration.	*Targeted Investment / Phased Rollout*	approx 0.45
Aggressive Adoption	Near-exponential early uptake driven by a national mandate and massive investment.	*National Priority / Security-Driven*	approx 0.70

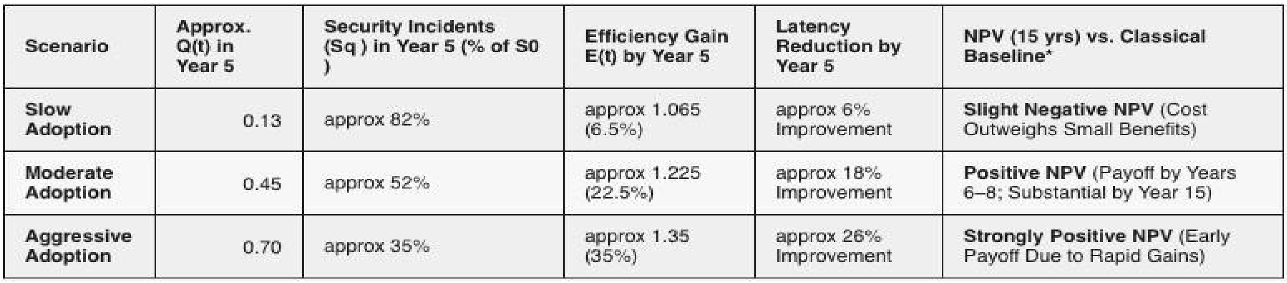
4. Empirical Estimation & Parameterization

We estimate parameters based on comparable sector data:

- α **(Security Reduction Factor):** Set $\alpha = \mathbf{1.5}$ for the moderate scenario. This implies a ~ 78% reduction in quantum-vulnerable incidents when $Q(t) = 1$.
- β **(Efficiency Gain Coefficient):** Set $\beta = \mathbf{0.5}$ for a moderate scenario, assuming an average 50% efficiency gain across optimization tasks [9].
- **Other Values:** Discount rate $r = 5\%$; Baseline security incidents $S_0 = 100$.

5. Projections and Predictive Analysis

Simulation outcomes over a 15-year horizon ($t = 1 \ldots 15$):



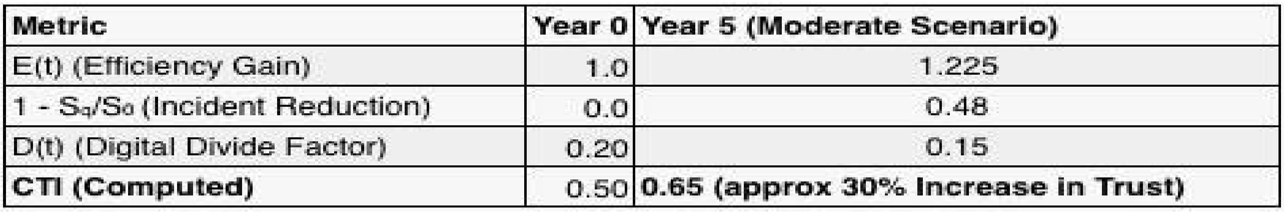
Scenario	Approx. Q(t) in Year 5	Security Incidents (Sq) in Year 5 (% of S0)	Efficiency Gain E(t) by Year 5	Latency Reduction by Year 5	NPV (15 yrs) vs. Classical Baseline*
Slow Adoption	0.13	approx 82%	approx 1.065 (6.5%)	approx 6% Improvement	**Slight Negative NPV** (Cost Outweighs Small Benefits)
Moderate Adoption	0.45	approx 52%	approx 1.225 (22.5%)	approx 18% Improvement	**Positive NPV** (Payoff by Years 6–8; Substantial by Year 15)
Aggressive Adoption	0.70	approx 35%	approx 1.35 (35%)	approx 26% Improvement	**Strongly Positive NPV** (Early Payoff Due to Rapid Gains)

In the Slow scenario, the cost of limited PQC/QC adoption fails to generate sufficient security-related cost savings or efficiency-based economic value, resulting in a net loss.

5.1 Impact on Citizen Trust (CTI)

Citizen trust $U(t)$ is modelled as a function of tangible benefits and the Digital Divide factor $D(t)$: $S_q(t)/S_0$) offset by the **Digital Divide/Inequality Factor** $D(t)$ inherent in new technologies:

$$\text{Citizen Trust Index (CTI)}(t) = U_0 + \gamma_1 \cdot E(t) + \gamma_2 \cdot (1 - S_q(t)/S_0) - \gamma_3 \cdot D(t)$$



Metric	Year 0	Year 5 (Moderate Scenario)
E(t) (Efficiency Gain)	1.0	1.225
1 - S_q/S_0 (Incident Reduction)	0.0	0.48
D(t) (Digital Divide Factor)	0.20	0.15
CTI (Computed)	0.50	**0.65 (approx 30% Increase in Trust)**

The results project a net increase in citizen trust of ~ 30% over five years, primarily driven by enhanced security and efficiency.

6. Discussion: Risks, Bottlenecks, and Strategic Caveats

Critical implementation challenges include:

- **Hardware Limitations:** Near-term efficiency is limited by the current NISQ (Noisy Intermediate-Scale Quantum) era devices.
- **Transition Risk:** The PQC migration period creates a window for **"Harvest Now, Decrypt Later"** attacks [10].

- **Regulatory Gaps:** The need for new governance frameworks to manage algorithmic opacity, fairness, and compliance with data privacy laws (e.g., GDPR).
- **Skill Gaps:** A global shortage of quantum expertise will slow the increase in $Q(t)$.

7. Policy Implications and Recommendations

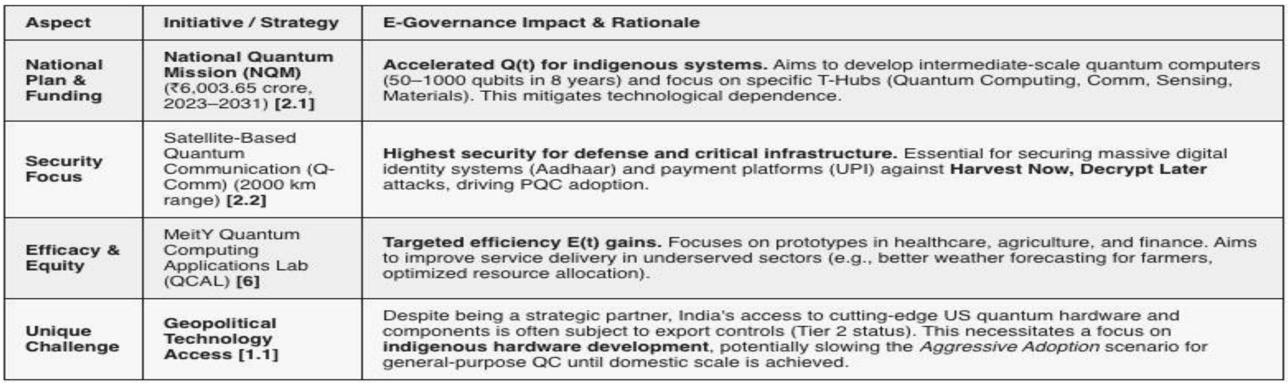
1. **Mandate PQC Migration Now:** Implement an **Aggressive** adoption strat- egy for quantum-resistant cryptography across all critical government systems.
2. **Invest in Hybrid Architecture:** Fund national labs and testbeds to build inter- nal competence and integrate quantum with existing HPC infrastructure.
3. **Establish Ethical Governance Frameworks:** Adopt principles of algorithmic transparency and fairness, potentially via a dedicated framework like the WEF's principles [11], to manage the risk of administrative opacity and secure public trust.
4. **Prioritize Digital Inclusion:** Ensure QC benefits extend to all demographic and regional segments to actively reduce the Digital Divide Factor $D(t)$.

8. Country-Specific E-Governance Strategies and Geopo- litical Dynamics

The efficacy of QC is significantly shaped by national policy and geopolitical positioning.

8.1 India: Focus on Digital Sovereignty and Inclusive Applica- tions

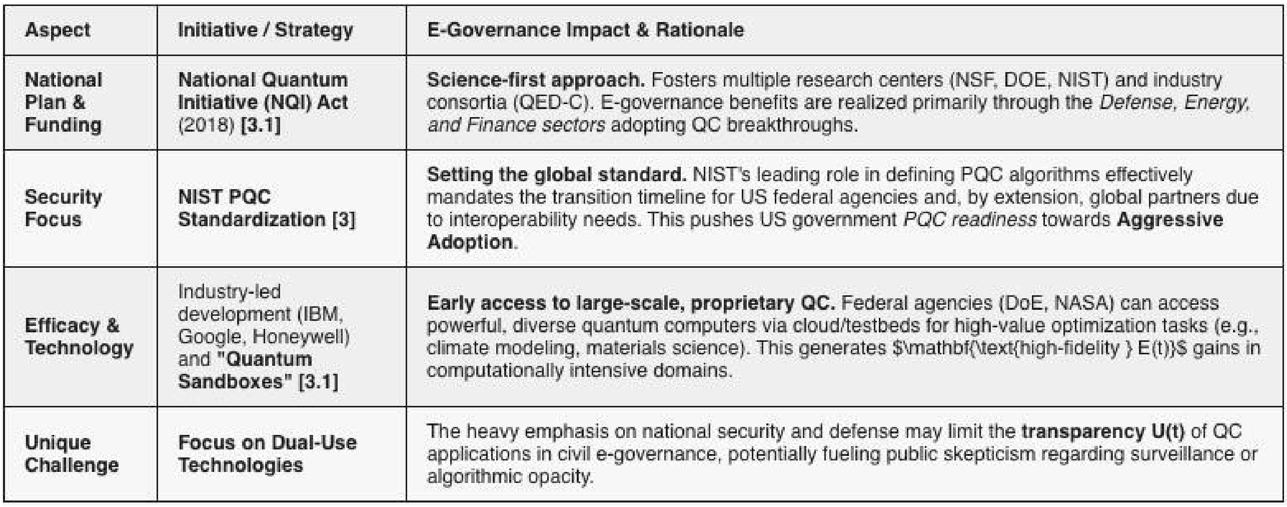
India's strategy, is driven by the principles of "Digital India and "Aatmanirbhar Bharat" emphasising indigenous development to ensure digital sovereignty and address the needs of a vast, diverse population. National Quantum Mission is the key focus.



Aspect	Initiative / Strategy	E-Governance Impact & Rationale
National Plan & Funding	**National Quantum Mission (NQM)** (₹6,003.65 crore, 2023–2031) **[2.1]**	**Accelerated Q(t) for indigenous systems.** Aims to develop intermediate-scale quantum computers (50–1000 qubits in 8 years) and focus on specific T-Hubs (Quantum Computing, Comm, Sensing, Materials). This mitigates technological dependence.
Security Focus	Satellite-Based Quantum Communication (Q-Comm) (2000 km range) **[2.2]**	**Highest security for defense and critical infrastructure.** Essential for securing massive digital identity systems (Aadhaar) and payment platforms (UPI) against **Harvest Now, Decrypt Later** attacks, driving PQC adoption.
Efficacy & Equity	MeitY Quantum Computing Applications Lab (QCAL) **[6]**	**Targeted efficiency E(t) gains.** Focuses on prototypes in healthcare, agriculture, and finance. Aims to improve service delivery in underserved sectors (e.g., better weather forecasting for farmers, optimized resource allocation).
Unique Challenge	**Geopolitical Technology Access [1.1]**	Despite being a strategic partner, India's access to cutting-edge US quantum hardware and components is often subject to export controls (Tier 2 status). This necessitates a focus on **indigenous hardware development**, potentially slowing the *Aggressive Adoption* scenario for general-purpose QC until domestic scale is achieved.

8.2 United States (US): Focus on National Security and Private Sector Lead

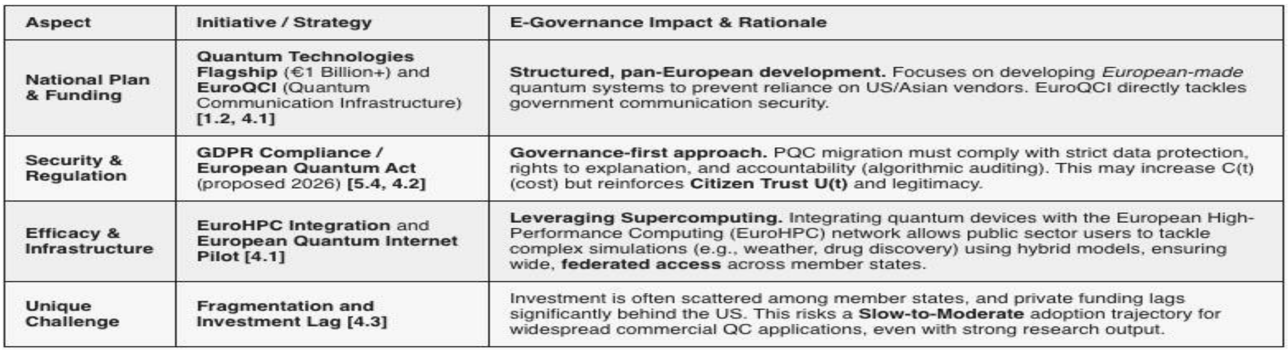
The US approach, driven by the **National Quantum Initiative (NQI)** [14], aims for technological supremacy and leverages a robust public-private ecosystem.



Aspect	Initiative / Strategy	E-Governance Impact & Rationale
National Plan & Funding	**National Quantum Initiative (NQI) Act** (2018) **[3.1]**	**Science-first approach.** Fosters multiple research centers (NSF, DOE, NIST) and industry consortia (QED-C). E-governance benefits are realized primarily through the *Defense, Energy, and Finance sectors* adopting QC breakthroughs.
Security Focus	**NIST PQC Standardization [3]**	**Setting the global standard.** NIST's leading role in defining PQC algorithms effectively mandates the transition timeline for US federal agencies and, by extension, global partners due to interoperability needs. This pushes US government *PQC readiness* towards **Aggressive Adoption**.
Efficacy & Technology	Industry-led development (IBM, Google, Honeywell) and **"Quantum Sandboxes" [3.1]**	**Early access to large-scale, proprietary QC.** Federal agencies (DoE, NASA) can access powerful, diverse quantum computers via cloud/testbeds for high-value optimization tasks (e.g., climate modeling, materials science). This generates $\mathbf{\text{high-fidelity } E(t)}$ gains in computationally intensive domains.
Unique Challenge	**Focus on Dual-Use Technologies**	The heavy emphasis on national security and defense may limit the **transparency U(t)** of QC applications in civil e-governance, potentially fueling public skepticism regarding surveillance or algorithmic opacity.

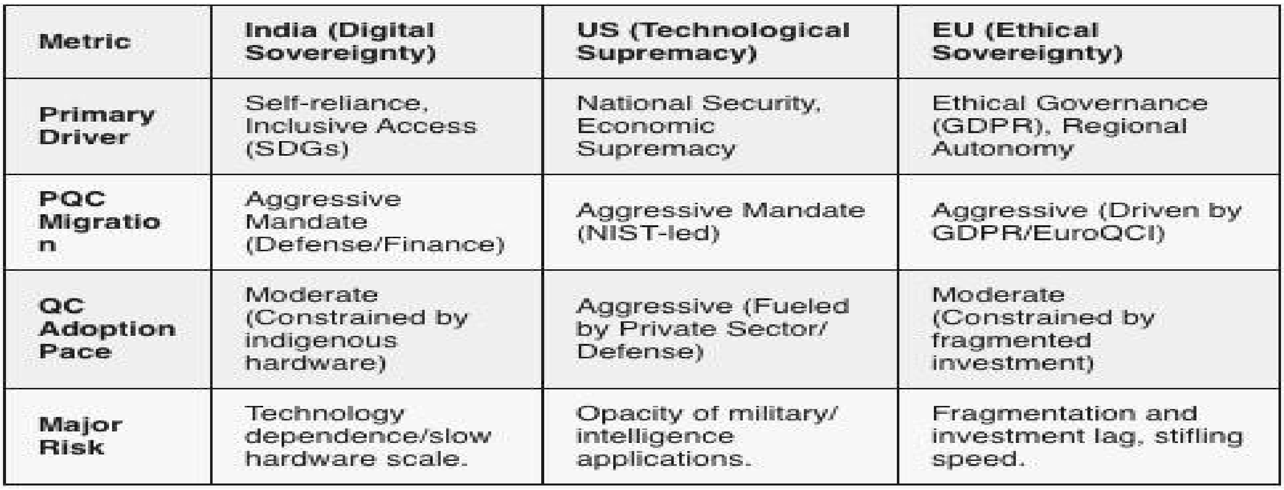
8.3 European Union (EU): Focus on Ethical Governance and **Sovereignty through Collaboration**

The EU strategy prioritizes **Technological Sovereignty** balanced by strong ethical and regulatory frameworks, notably the forthcoming **European Quantum Act** [15].



Aspect	Initiative / Strategy	E-Governance Impact & Rationale
National Plan & Funding	**Quantum Technologies Flagship** (€1 Billion+) and **EuroQCI** (Quantum Communication Infrastructure) **[1.2, 4.1]**	**Structured, pan-European development.** Focuses on developing *European-made* quantum systems to prevent reliance on US/Asian vendors. EuroQCI directly tackles government communication security.
Security & Regulation	**GDPR Compliance / European Quantum Act** (proposed 2026) **[5.4, 4.2]**	**Governance-first approach.** PQC migration must comply with strict data protection, rights to explanation, and accountability (algorithmic auditing). This may increase C(t) (cost) but reinforces **Citizen Trust U(t)** and legitimacy.
Efficacy & Infrastructure	**EuroHPC Integration** and **European Quantum Internet Pilot [4.1]**	**Leveraging Supercomputing.** Integrating quantum devices with the European High-Performance Computing (EuroHPC) network allows public sector users to tackle complex simulations (e.g., weather, drug discovery) using hybrid models, ensuring wide, **federated access** across member states.
Unique Challenge	**Fragmentation and Investment Lag [4.3]**	Investment is often scattered among member states, and private funding lags significantly behind the US. This risks a **Slow-to-Moderate** adoption trajectory for widespread commercial QC applications, even with strong research output.

8.4 Comparative Summary



Metric	India (Digital Sovereignty)	US (Technological Supremacy)	EU (Ethical Sovereignty)
Primary Driver	Self-reliance, Inclusive Access (SDGs)	National Security, Economic Supremacy	Ethical Governance (GDPR), Regional Autonomy
PQC Migration	Aggressive Mandate (Defense/Finance)	Aggressive Mandate (NIST-led)	Aggressive (Driven by GDPR/EuroQCI)
QC Adoption Pace	Moderate (Constrained by indigenous hardware)	Aggressive (Fueled by Private Sector/ Defense)	Moderate (Constrained by fragmented investment)
Major Risk	Technology dependence/slow hardware scale.	Opacity of military/ intelligence applications.	Fragmentation and investment lag, stifling speed.

9. Conclusion

Quantum computing offers promising efficacy for e-governance and the public sector. Our predictive models show that with **moderate to aggressive adoption**, the benefits (reduced breach risks, higher efficiency, increased trust) can outweigh the costs within ~ 5− 10years. To fully realize benefits, governments must execute a dual strategy: a rapid, non-negotiable migration to PQC, coupled with a sustainable, ethically governed investment in QC infrastructure and skill development.

References

1. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 39(3), 511-538
2. National e-Governance Division (NeGD), Government of India. (2024).MeitY Quan- *tum Computing Applications Lab (QCAL)*. [Available online at the official NeGD website].
3. Quantum Technology and Application Consortium (QUTAC). (Year). Industry
4. quantum computing applications. *EPJ Quantum Technology*.
5. Boston Consulting Group (BCG). (2024).Quantum Computing On Track to Create *Up to US$ 850 Billion of Economic Value By 2040.* [Report, available online at the BCG website].

6. Quantum computing and cybersecurity: a rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019–2024). *Discover Ap- plied Sciences*, 2025.
7. Practical Quantum K-Means Clustering: Performance Analysis and Ap-
8. **plications in Energy Grid Classification.** ***arXiv preprint*.**
9. National Academies of Sciences, Engineering, and Medicine.(2019).
10. ***Quantum Computing: Progress and Prospects*** **. National Academies Press.**
11. The World Economic Forum. (2022).Quantum Computing Governance
12. ***Principles.*** **[Report, available online at the WEF website].**
13. Government of India, Department of Science & Technology. (2023).National Quantum Mission (NQM).Approved by the Union Cabinet. [Press **Release/Official Document].**
14. Joe, S. (2025). America’s Quantum Shield vs. India’s Digital Sovereignty.
15. ***Medium*.**
16. U.S. Congress. (2018).NationalQuantumInitiativeAct.Public Law 115 - 368
17. European Commission. (2025).European Quantum Strategy and Quantum Technologies Flagship.[Official Policy Document].
18. DigitalEurope. (2025).Making Europe a quantum industry powerhouse: A strategic EU roadmap for investment, talent and industrial scale.
19. MeitY Quantum Computing Applications Lab] Nationale-Governance Division Government of India.
20. The future of quantum computing for the public sector. [Reference for skills/cost analysis]
21. Secure Public Engagement using Quantum-Computing Integrated Digital Interaction: Cryptography and Blockchain. Atlantis Press.
22. Vyas, K., et al. (Year). The Impact of Quantum Computing on Cryptography: Opportunities and Challenges. International Journal of Intelligent Systems and Applications in Engineering.
23. National Institute of Standards and Technology (NIST). (2024). Post-Quantum Cryptography Standardization. Status Report. Gaithersburg,
24. MD: U.S. Department of Commerce.
25. Montanaro, A. (2016). Quantum algorithms for graph problems. Quantum Information & Computation 16(5-6), 405-430
26. Nasscom projects quantum techologies to add US$ 280 - 310 billion to India's economy by 2030.