Journal of Liberty and International Affairs · Volume 12 · Number 2 · 2026 · eISSN 1857-9760
Published online by the Institute for Research and European Studies at www.e-jlia.com

Copyright © 2026 The author/s
This work is licensed under the CC BY 4.0 license
(*) Corresponding author
Peer review method: Double-blind
Research article
DOI: https://doi.org/10.47305/jlia.2026.2373
Received: 08.04.2025 • Accepted after revision: 10.09.2026 • Published: 23.09.2026
Pages: 165-185

Technological Sovereignty and the New Digital Geopolitics: Comparative Quantum Governance in China, the United States, and the European Union

Daniele Battista[1*], Arthur A. S. Gugliucciello[2], Alessandra Petrone[3]

[1]University of Salerno - Fisciano (SA), Italy ✉ dbattista@unisa.it
[2]University of Salerno - Fisciano (SA), Italy ✉ arthurasgugliucciello@gmail.com
[3]University of Salerno - Fisciano (SA), Italy ✉ apetrone@unisa.it

Abstract
How do institutional differences shape the governance of quantum technologies? Comparing China, the United States, and the European Union through a structured, focused comparison of policy documents and standards (2018–2026), this article investigates governance pathways. It develops a configurational framework based on a strategic triangle of state direction, market coordination, and standard-setting capacity. Findings reveal three distinct hybrid trajectories: concentrated state direction in China; mission-oriented federal coordination with market dynamism in the United States; and multilevel normative coordination coupled with an industrial turn in the European Union. These configurations generate critical trade-offs across resource mobilization, commercialization, transparency, and interoperability. Finally, the article advances an operational comparative model and proposes a polycentric governance architecture centered on technical standards, post-quantum cryptographic migration, anticipatory review, and confidence-building measures.

Keywords
Quantum Governance; Comparative Political Economy; Technological Sovereignty; Post-Quantum Cryptography; International Standards

UN Sustainable Development Goals (SDGs)
SDG 9: Industry, Innovation and Infrastructure; SDG 16: Peace, Justice and Strong Institutions; SDG 10: Reduced Inequalities

INTRODUCTION

Each case combines public authority, firms, universities, standards organizations, and security institutions. The comparative task is therefore to identify which mechanism is dominant, how the mechanisms interact, and what consequences follow from that configuration.

Against this background, the article asks: How does the allocation of steering capacity among state institutions, market actors, and normative or standard-setting bodies shape quantum technology governance in China, the United States, and the European Union, and what forms of international coordination follow from these differences? The article argues that the three cases are hybrid but systematically distinct. China's configuration privileges concentrated state direction; the United States combines market coordination with an increasingly explicit mission-oriented federal role; and the European Union relies on multilevel public coordination and normative capacity while moving toward a stronger industrial and security policy. These configurations help explain variation in resource mobilization, commercialization, interoperability, transparency, and strategic autonomy. The article contributes by

operationalizing the strategic triangle of state, market, and norms as a structured comparative framework, applying it to a common body of indicators, and deriving concrete proposals for multilevel governance rather than invoking global regulation in the abstract.

The question has a social and democratic dimension as well as an industrial one. Decisions about who may access public machines, which applications receive funding, how security exceptions are defined, and whose expertise is represented in standards processes distribute both opportunity and authority. Early institutional choices can become difficult to reverse because research facilities, procurement contracts, training pipelines, and technical interfaces create path dependence. A governance analysis must therefore examine not only national competitiveness, but also the conditions under which quantum infrastructures acquire legitimacy and social value. This is especially important in a field where technical complexity can narrow public scrutiny and where narratives of inevitability may substitute for evidence. The article responds by treating transparency, access, and responsibility as observable features of governance rather than as rhetorical additions to technological strategy. Broader scholarship on AI-mediated political communication also illustrates how emerging technologies acquire public significance through institutional framing and expectations, even though quantum governance presents distinct infrastructural, dual-use, and standard-setting challenges (Battista, 2024; Battista and Mangone, 2025).

THEORETICAL FRAMEWORK: INSTITUTIONAL CONFIGURATIONS OF QUANTUM GOVERNANCE

Emerging-Technology Governance as Sociotechnical Ordering

The primary theoretical perspective is the institutional political economy of innovation, complemented by science and technology studies (STS) on large technical systems and path dependence. Quantum capability is not produced by hardware in isolation: it depends on laboratories, fabrication and cryogenic facilities, specialist workforces, supply chains, public funding, standards, procurement, and security institutions that evolve together. Hughes's large-technological-systems approach is useful because it treats technical artifacts, organizations, scientific knowledge, finance, and regulation as components of a single sociotechnical configuration (Hughes, 1987). The framework also incorporates the possibility of technological lock-in: increasing returns, accumulated expertise, installed infrastructure, and standard-setting can make early technical and institutional choices progressively costly to reverse (Arthur, 1989).

This STS perspective aligns directly with emerging scholarship on quantum technology governance. Quantum technologies are already embedded in policy programs that connect scientific development with social expectations, responsible innovation, infrastructure access, and security, even though large-scale applications remain uncertain (Coenen et al., 2022; Perrier, 2022; Atladottir et al., 2025). The analytical implication is that governance must be studied as the co-production of technical capability and institutional order. Decisions about which facilities are financed, which benchmarks are recognized, who gains access to experimental machines, and which applications are classified as strategic help shape the technological trajectory rather than merely regulate it after the fact.

CC BY

A second foundation concerns standards and anticipatory governance. In immature technological fields, standards can coordinate expectations before dominant architectures have stabilized, but they can also create path dependence by privileging specific interfaces, performance criteria, or cryptographic baselines. Recent quantum-governance scholarship therefore emphasizes responsive and standards-oriented instruments that can preserve innovation while creating common expectations for interoperability, responsibility, and security (Aboy et al., 2025; Ten Holter, Inglesant, and Jirotka, 2023). Normative capacity is consequently treated here as a productive form of governance: its importance lies not only in declaring principles, but in translating them into auditable procedures, technical standards, procurement requirements, reviewable exceptions, and mechanisms for cross-border coordination.

A third foundation is the political economy of high-capital and dual-use infrastructures. Quantum computing requires long investment horizons, scarce expertise, costly facilities, and sustained public support, while quantum communication, sensing, and cryptographic applications cross civilian, commercial, and security domains. Research on dual-use technology shows that civilian and military trajectories are linked through funding, procurement, knowledge transfer, and industrial organization rather than through a simple division between separate technological sectors (Molas-Gallart, 1997). In quantum systems, these dynamics interact with public financing of uncertain innovation (Mazzucato and Semieniuk, 2017), cryptographic and national-security concerns (Hoofnagle and Garfinkel, 2022), and strategic dependencies created by transnational technical networks (Farrell and Newman, 2019). This combination makes the allocation of steering capacity among state institutions, firms, and standards bodies a central explanatory problem.

Taken together, these literatures yield three propositions for the comparison. First, quantum capability is sociotechnically assembled, so institutional coordination and infrastructure matter alongside scientific performance. Second, early investments and standards can produce path dependence, making the timing and location of governance consequential. Third, the field's high capital intensity and dual-use character make public authority, market experimentation, and normative coordination mutually dependent rather than substitutable. The strategic triangle developed below operationalizes these propositions by asking how each jurisdiction distributes steering capacity among the state, market actors, and normative or standard-setting institutions, and what trade-offs this configuration generates for mobilization, commercialization, interoperability, transparency, security, and access.

The Strategic Triangle: Dimensions, Mechanisms, and Expectations

Within this perspective, the strategic triangle specifies three analytically distinct dimensions. First, state direction refers to the capacity of public authorities to set priorities, concentrate resources, build infrastructure, coordinate agencies, use procurement, and connect research to security or industrial missions. Mann's (1984) concept of infrastructural power is useful here as a bounded component of the framework: it captures the ability to implement decisions through organizational and knowledge networks, not merely to announce a strategy. The observable indicators are the presence of a durable national or supranational strategy, coordinating bodies, mission-oriented funding, public research infrastructure, and implementation instruments.

CC BY

Second, market coordination concerns the extent to which firms, venture capital, intellectual-property regimes, and university-industry networks select technological pathways and organize commercialization. Market coordination does not imply an absent state. Public finance can create markets and absorb early uncertainty, while private actors provide experimentation, scaling, and application-specific knowledge (Edler and Fagerberg, 2017; Mazzucato and Semieniuk, 2017). The relevant indicators are the autonomy and density of firms, access to risk capital, commercialization pathways, technology transfer, and the use of public-private partnerships.

Third, normative and standard-setting capacity is the ability to translate political values and technical choices into rules that structure other actors' behavior. It includes interoperability and performance standards, cryptographic baselines, ethical principles, access provisions, and mechanisms for cross-border coordination. In the EU case, the notion of normative power identifies a specific pathway through which rule-making can produce external influence (Manners, 2002); it is treated here as a case-level mechanism rather than as a separate general theory. Standards also have geopolitical effects because control over technical architectures can create dependencies and coercive leverage within transnational networks (Farrell and Newman, 2019; Zuniga et al., 2024).

The triangle is therefore configurational, not categorical. A case is represented by the relative strength and interaction of the three dimensions, and its position may change over time. The framework generates three conditional expectations. Concentrated state direction should support rapid resource mobilization and long-term missions, but may weaken transparency, contestation, and independent validation. Strong market coordination should accelerate experimentation and commercialization, but can fragment standards and underprovide public goods such as workforce development or cryptographic migration. Strong normative capacity should improve interoperability, legitimacy, and anticipatory oversight, but may not by itself solve financing and scale-up problems. These expectations guide the comparison; they do not predetermine technological performance.

Institutional configurations can also generate feedback. A public research mission may create firms and specialist labor markets, thereby strengthening the market vertex; a commercially successful platform may induce procurement rules and security controls, strengthening state direction; and a technical standard may lower entry costs, enabling new market participants while expanding the authority of the standards body. Conversely, incompatibility among benchmarks, export controls, and national security classifications can pull a configuration toward closure. The triangle is thus designed to capture both the initial distribution of steering capacity and the subsequent co-evolution of its dimensions. This dynamic interpretation is necessary for a technology whose governance is developing before stable commercial architectures have emerged.

RESEARCH DESIGN AND METHODOLOGY

The study uses a qualitative, structured-focused comparison (George and Bennett, 2005). The comparison is structured because the same questions and indicators are applied to each case; it is focused because it examines the governance of quantum computing and closely connected quantum infrastructures rather than attempting to measure the entire field of

CC BY

quantum science. The design is explanatory and typological: it identifies institutional mechanisms that make different policy trajectories plausible. It does not claim to estimate the causal effect of a single variable or to rank national technological performance.

China, the United States, and the European Union were selected because they are central poles in the emerging quantum ecosystem and exhibit markedly different allocations of authority across public institutions, firms, and supranational bodies. Their inclusion therefore offers analytical leverage for examining institutional variation under a shared strategic pressure. The EU is treated as a multilevel polity rather than as a state; member-state diversity is incorporated as a feature of its coordination problem. The observation window runs from January 2018, when the United States enacted the National Quantum Initiative Act, through 31 July 2026. This period captures the shift from broad research strategies toward industrialization, security policy, infrastructure deployment, and post-quantum cryptographic implementation.

The evidence base combines peer-reviewed research with authoritative policy documents. Materials were identified through targeted searches of official repositories maintained by the three jurisdictions and by organizations directly involved in quantum governance, including quantum.gov, NIST, the European Commission, EuroHPC, the OECD, ITU, ISO/IEC, and official English-language Chinese government portals. Documents were included when they (1) explicitly addressed quantum technologies; (2) specified governance objectives, institutions, funding or implementation mechanisms; (3) fell within the observation window or remained institutionally operative during it; and (4) were attributable to a public authority, standards body, or peer-reviewed publication. Corporate announcements and industry news were excluded from the core comparative evidence and used only when no public source existed for a narrowly factual technological announcement.

Data extraction followed a common matrix with five dimensions: state direction; market coordination; normative and standard-setting capacity; the balance between openness and security; and observable governance outcomes and constraints. Each case was examined through the same questions: Who sets priorities? How are resources mobilized? Which actors control commercialization? How are standards and responsibilities defined? Which implementation outputs are visible, and what institutional bottlenecks remain? Within-case evidence was first organized chronologically and then compared across dimensions. Claims based on patents, startups, or investment are interpreted as partial ecosystem indicators rather than as equivalent measures of usable quantum capability. This procedure directly addresses the metric incommensurability that can otherwise distort cross-case comparison. Document extraction and coding were conducted manually by the authors using the structured five-dimensional matrix; no CAQDAS package or automated text-classification procedure was used. The matrix functioned as a common coding sheet and audit trail across the three cases.

Three quality controls were applied. Source triangulation required strategic claims to be supported, where possible, by both an authoritative institutional document and independent scholarly analysis.

Temporal bracketing distinguished enacted or implemented measures from announced future initiatives; proposals such as a forthcoming legislative instrument were not coded as existing law. Finally, rival interpretations were retained when the same instrument could support more than one vertex of the triangle. For example, a public-private consortium is evidence of state direction and market coordination, while a cryptographic standard may simultaneously

CC BY

reflect public authority, technical expertise, and market implementation. This prevents the framework from forcing hybrid evidence into a single category and strengthens the credibility of the explanatory comparison.

STRATEGIC SIGNIFICANCE WITHOUT TECHNOLOGICAL DETERMINISM

Quantum computing is strategically relevant because certain algorithms, if executed on a sufficiently large and fault-tolerant machine, could affect public-key cryptography, optimization, simulation, and scientific discovery. Yet the transition from experimental devices to reliable, general-purpose capability remains uncertain and problem-specific. Quantum advantage in one benchmark does not establish broad economic or military superiority, and qubit counts alone do not capture fidelity, error correction, connectivity, software, or usable workloads. The appropriate analytical stance is therefore conditional: quantum systems may alter selected capabilities, but the timing, scale, and distribution of those effects depend on complementary institutions and infrastructures.

Cryptography illustrates why governance cannot simply wait for technical maturity. Migration from vulnerable public-key systems can take many years, while sensitive data may be collected today for later decryption. This temporal mismatch creates a present coordination problem even in the absence of a cryptographically relevant quantum computer (Mosca, 2018; Hoofnagle and Garfinkel, 2022). NIST's finalization of FIPS 203, 204, and 205 in 2024 converted a prospective risk into implementable technical baselines (NIST, 2024a, 2024b, 2024c). The strategic issue is thus not only who builds the most powerful machine, but who develops standards, inventories vulnerable systems, coordinates procurement, prepares workforces, and distributes transition costs.

The same caution applies to claims about a technological arms race. Competition is visible in investment, export controls, research security, and standard-setting, but quantum innovation also relies on transnational scientific communities, supply chains, and interoperable infrastructures. Competition and interdependence coexist. The governance challenge is to preserve legitimate security protections without converting every scientific exchange into a zero-sum contest. This tension provides the common strategic environment within which the three institutional configurations operate.

Although the empirical emphasis is quantum computing, communication and sensing remain part of the governance environment. Quantum networks raise questions about interoperability, infrastructure ownership, and cross-border security; sensing applications intensify dual-use concerns; and post-quantum cryptography affects conventional digital systems rather than quantum hardware alone. These domains are included when they reveal the institutional logic of a case, but they are not aggregated into a single performance score. The bounded scope keeps the comparison analytically coherent while acknowledging that quantum strategies increasingly treat computing, communication, sensing, enabling technologies, and skills as an interconnected portfolio.

CC BY

Comparative Analysis of Governance Configurations

The comparison applies the five-dimensional matrix to all three cases. It deliberately separates governance capacity from technological performance: an institutional configuration can mobilize resources effectively while remaining opaque, produce commercially visible firms while underproviding coordination, or generate sophisticated rules without achieving industrial scale. The analysis therefore asks how each configuration converts authority and resources into policy outputs, and which trade-offs recur.

China: Concentrated Direction and Strategic Integration

China's quantum policy is anchored in concentrated state direction. The Fourteenth Five-Year Plan placed quantum information among the frontier fields around which national laboratories, basic research, and strategic scientific capacity were to be organized (State Council of the People's Republic of China, 2021). Priority-setting is linked to technological self-reliance, industrial policy, and national security. This configuration gives central authorities the capacity to sustain long time horizons, coordinate major facilities, and align research agendas with broader state objectives. In terms of the framework, state direction is the primary mechanism because public institutions define missions and structure the environment within which universities, laboratories, and firms operate.

Market coordination is present but supporting rather than autonomous. Private and nominally private firms contribute engineering, commercialization, and application development, yet public priorities strongly condition access to finance, infrastructure, and strategic projects. This hybrid form should not be reduced to a command system: competition among localities, research organizations, and firms can generate experimentation. Nevertheless, the allocation of resources and the security sensitivity of parts of the field give the state a greater capacity to select trajectories than in the other cases. The resulting advantage is organizational concentration; the corresponding risk is that political alignment can narrow independent evaluation and make unsuccessful pathways harder to identify publicly.

China also treats standards and intellectual property as instruments of technological sovereignty. Experience in telecommunications shows an increasingly active effort to connect domestic innovation with participation in international standard-setting (Kim, Lee, and Kwak, 2020). In the quantum field, however, standards influence should not be inferred directly from patent counts. Applications, granted patents, scientific publications, prototype performance, and deployable systems measure different phenomena. The EPO/OECD's multidimensional mapping reinforces the need to assess innovation, firms, investment, skills, trade, and policy together rather than to equate filing volume with operational leadership (EPO/OECD, 2025).

The causal mechanism is resource concentration under a national mission. It supports infrastructure building and coordinated research, but also produces an evidence problem: public data about funding, security-linked programs, negative results, and institutional performance are less complete and less easily comparable. This opacity limits external validation and complicates claims of supremacy. China's configuration is therefore best understood as high steering capacity combined with selective market mobilization and strategically oriented

CC BY

standards participation. Its observable strength is continuity; its principal governance constraint is the tension between strategic control, transparency, and broad-based access.

The openness-security dimension makes this trade-off particularly visible. International collaboration and standards participation can accelerate learning and confer legitimacy, while self-reliance policies and security classification limit knowledge flows. The two tendencies are not contradictory: they are selective instruments within the same strategy. China can support openness in forums where interoperability or market access advances national capacity and restrict openness where authorities perceive strategic vulnerability. The expected outcome is neither isolation nor unrestricted integration, but managed interdependence. For comparative purposes, this explains why participation in global institutions should be evaluated together with domestic access rules and disclosure practices.

United States: Market Dynamism Within a Mission-Oriented State

The United States has the strongest market-coordination component, but describing it as market-led obscures the public architecture that makes the ecosystem possible. The National Quantum Initiative Act established a coordinated federal program, authorized research centers and consortia, and formalized collaboration among agencies, national laboratories, universities, and industry (United States Congress, 2018). The National Quantum Coordination Office, the Subcommittee on Quantum Information Science, and the National Quantum Initiative Advisory Committee provide networked rather than centralized steering. Federal institutions finance basic research, develop measurement and standards capacity, train workers, and create demand, while firms and universities retain substantial autonomy over technological pathways (NSTC, 2024).

Market coordination is primary in commercialization. Venture finance, corporate research, cloud access, and university-industry transfer enable multiple hardware and software approaches to compete. This diversity can accelerate experimentation and attract talent. However, it also creates fragmentation: benchmarks may be vendor-specific, incentives favor visible milestones, and public-interest tasks with diffuse returns can be delayed. The state's role is consequently mission-oriented rather than residual. It reduces uncertainty, funds shared infrastructure, protects strategically sensitive knowledge, and uses procurement and technical standards to coordinate actors that would otherwise optimize locally.

The post-quantum cryptography transition demonstrates the interaction between market and state. NIST organized an international evaluation process and issued implementation-ready FIPS standards in 2024. Executive Order 14412 subsequently required strategic coordination of federal migration and set implementation responsibilities across OMB, NIST, CISA, and the Office of the National Cyber Director (The White House, 2026a). Executive Order 14413 also called for an updated national strategy and a whole-of-government effort covering research, manufacturing, commercialization, and application (The White House, 2026b). These measures qualify the assumption that U.S. leadership emerges from markets alone: public authority supplies standards, deadlines, security priorities, and coordination.

The causal mechanism is decentralized experimentation nested within federal missions. Its observable strengths are commercialization capacity, technical standard-setting, and the ability to connect public research with private scaling. Its constraints are interagency fragmentation, uneven adoption across critical infrastructure, and the possibility that proprietary

CC BY

incentives weaken interoperability or public scrutiny. The United States therefore occupies a position between the market and state vertices of the triangle, with particularly strong normative capacity in technical standards but a less integrated approach to social and ethical governance.

Federal coordination also operates through specialized institutional roles rather than a single ministry. The NQI framework assigns research, measurement, workforce, security, and international cooperation to different agencies and coordinating bodies (NSTC, 2024). This division permits expertise and portfolio diversity, but it raises transaction costs when responsibilities overlap or when migration depends on actors outside federal control. The NQIAC's work on quantum networking illustrates an advisory mechanism that connects industry, universities, laboratories, and government while identifying standards and infrastructure needs (NQIAC, 2024). The U.S. configuration therefore converts pluralism into capacity only when coordination offices, shared metrics, and procurement expectations align among otherwise autonomous actors.

European Union: Normative Coordination and an Emerging Industrial Turn

The European Union presents a multilevel configuration in which authority is divided among EU institutions, member states, research organizations, and firms. Its early comparative advantage lay in scientific networks, public research programs, and the capacity to coordinate across borders. The Quantum Europe Strategy adopted in July 2025 made the industrial turn explicit by linking research excellence to infrastructure, startup and scale-up support, supply-chain resilience, dual-use capability, and skills (European Commission, 2025). This is not a purely regulatory agenda; it combines normative coordination with a more assertive effort to build sovereign capacity.

State direction is strong but dispersed. The European Commission can set strategic priorities and mobilize common programs, while implementation remains dependent on member-state budgets, national institutions, and negotiated competencies. EuroHPC illustrates the benefits of this arrangement: by June 2026, the Joint Undertaking reported six procured quantum computers and a growing set of hybrid quantum-HPC infrastructures distributed across Europe (EuroHPC Joint Undertaking, 2026). Shared access can reduce duplication, broaden the user base, and turn public infrastructure into a platform for research and industrial learning. At the same time, multilevel bargaining can slow decisions and complicate the concentration of resources required for scale-up.

Normative and standard-setting capacity remains the EU's distinctive mechanism. Interoperability, data protection, security, responsible innovation, and cross-border access are treated as components of strategic autonomy rather than as constraints external to innovation. This orientation is consistent with the EU's broader ability to exert influence through rules and standards (Manners, 2002; Zuniga et al., 2024). Yet normative power is effective only when supported by technical competence, market presence, and implementation capacity. Rules written without domestic industrial depth may shape behavior but cannot guarantee leadership in hardware, software, or supply chains.

The causal mechanism is multilevel coordination through common programs and normative integration. Its strengths are legitimacy, transnational pooling, infrastructure access, and the capacity to connect responsible innovation with industrial policy. Its constraints are

CC BY

fragmented capital markets, uneven member-state capacity, and a persistent gap between excellent research and firm-level scaling. The EU therefore lies between the norms and state vertices of the triangle, while deliberately strengthening the market dimension. Its trajectory is one of partial convergence with the other cases, not regulatory exceptionalism.

The openness-security balance is expressed through shared research infrastructures, cross-border access, and an increasing concern with sovereign and dual-use capacity. The Quantum Europe Strategy places scientific openness alongside supply-chain resilience, space, security, and defense (European Commission, 2025). This combination can be productive if access conditions, research-security reviews, and industrial support are coordinated. It can also create tension when member states apply different security thresholds or when European preference conflicts with international collaboration. The EU's distinctive test is therefore implementation: whether normative commitments can be translated into common technical requirements and investment decisions across a heterogeneous polity.

Cross-Case Findings: Operationalizing the Strategic Triangle

The cross-case comparison yields three findings. First, the three configurations differ less in whether the state intervenes than in how public authority is organized. China concentrates direction within a national mission; the United States distributes it across agencies and public-private networks; the EU disperses it across supranational and member-state institutions. This allocation of authority shapes implementation. Concentration favors continuity and resource mobilization, networked federalism favors experimentation and technical specialization, and multilevel governance favors pooling and legitimacy while increasing coordination costs.

Second, the cases are converging around security, industrial policy, and standards, but they converge from different starting points. China combines state planning with selective firm participation and strategic standards engagement. The United States has reinforced public missions around an ecosystem still driven by private commercialization. The EU has supplemented its normative orientation with infrastructure, supply-chain, and dual-use policies. The triangle therefore captures relative emphasis and institutional interaction rather than fixed national identities.

Third, governance outcomes are complementary as well as competitive. No case simultaneously maximizes concentrated direction, decentralized experimentation, transparency, interoperability, and inclusive access. The policy problem is not to identify a universally superior model, but to understand which deficits each configuration must correct. Table 1 translates the triangle into a common analytic matrix and summarizes the mechanism, observable outcome, and principal constraint for each case.

The balance between openness and security cuts across all three findings. China manages openness selectively under a sovereignty-centered mission; the United States relies on open scientific and commercial networks while expanding research-security and cryptographic obligations; and the EU combines cross-border pooling with an agenda of strategic autonomy. In each case, security can supply resources and political urgency, but excessive securitization can reduce collaboration, independent testing, and public accountability. The framework therefore treats openness and security as a relationship to be governed, not as opposite endpoints on a universal scale.

CC BY

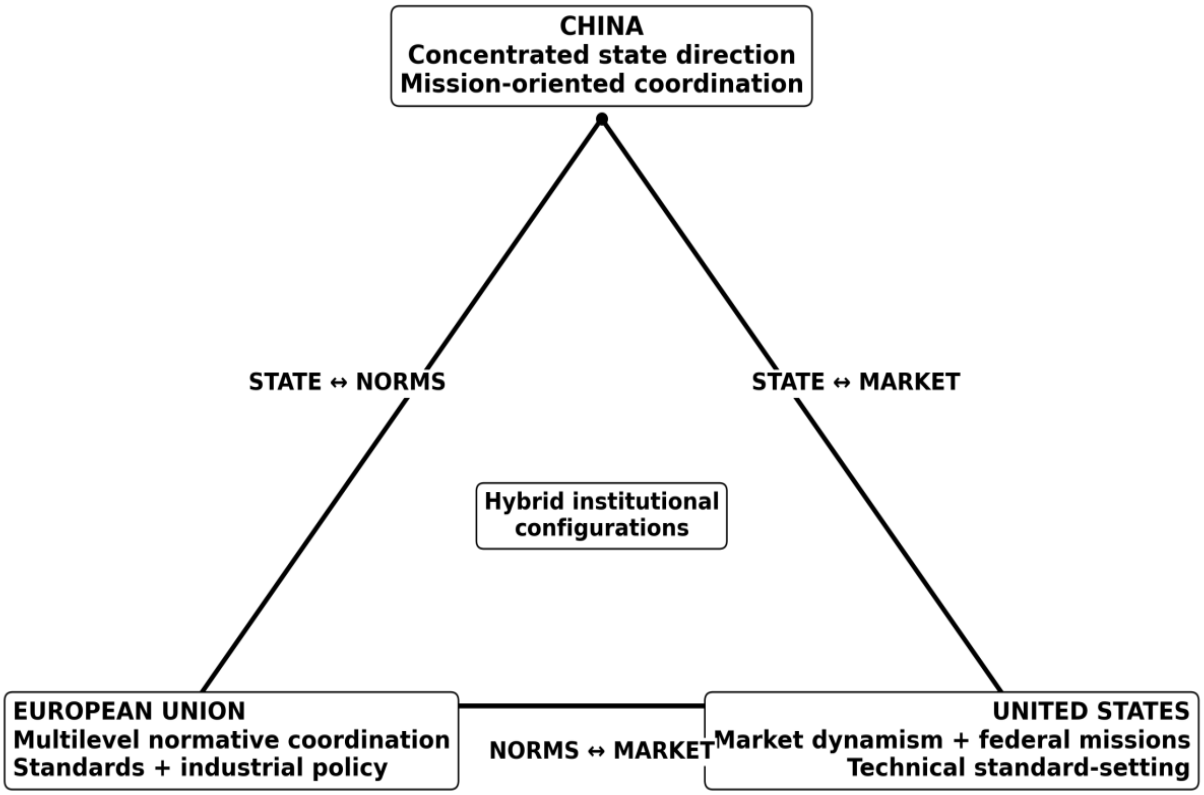


Figure 1: Strategic Triangle of Quantum Governance. The vertices denote dominant, not exclusive, coordination mechanisms (Source: Authors' elaboration)

Figure 1 should be read as a heuristic map. State, market, and norms are dimensions that coexist within every jurisdiction. Movement within the triangle can occur when policy instruments change: a procurement program strengthens state direction; venture formation strengthens market coordination; a binding standard or interoperability regime strengthens normative capacity. This interpretation transforms the model from a descriptive label into an analytical tool that can be applied longitudinally and to additional cases.

CC BY

Table 1: Structured Comparison of Quantum Governance Configurations (Source: Authors' elaboration)

Case	State Direction	Market Coordination	Norms and Standards	Mechanism, Outcome, and Principal Constraint
China	Primary: concentrated priority-setting, public laboratories, and security-linked missions	Supporting: firms operate within a state-shaped ecosystem	Strategic: standards participation supports technological sovereignty	Concentrated authority mobilizes resources and sustains long time horizons; opacity and limited comparability constrain external validation and broad participation.
United States	Strong but networked: federal missions coordinate agencies, laboratories, universities, and procurement.	Primary: private firms, venture finance, and university-industry transfer	Strong in technical standards, especially through NIST; less centralized in social and ethical governance	Public missions reduce uncertainty while firms commercialize; this produces scale and technical standards, but also fragmentation and uneven implementation across sectors.
European Union	Strong but multilevel: EU institutions and member states share authority and infrastructure.	Developing: vibrant research and startup base, with persistent scale-up and capital gaps	Primary: interoperability, rights, responsible innovation, and supranational standard-setting	Regulatory coordination and shared infrastructure create legitimacy and access; fragmented competencies and slower industrial scaling limit strategic autonomy.

Note: "Primary," "Strong," "Supporting," and "Developing" are qualitative descriptors based on the common documentary indicators outlined in the section entitled "Research Design and Methodology"; they are not numerical measures of technological performance.

FROM GENERAL APPEALS TO MULTILEVEL GOVERNANCE

The comparison suggests that a single global quantum regulator is neither realistic nor desirable at the present stage. Capabilities remain heterogeneous, security interests diverge, and technical standards are still evolving. A more feasible architecture is polycentric and modular: different institutions should govern the problems for which they possess authority and expertise, while common reporting and coordination prevent incompatible regimes (Radu, 2019). Four mechanisms are immediately actionable.

First, technical interoperability and terminology should be coordinated through existing standards bodies. ISO/IEC JTC 3, created in 2024 specifically for quantum technologies, provides a cross-domain venue for standards on computing, simulation, metrology, detectors, sources, and communication (ISO/IEC, 2024). For network applications, ITU-T Study Groups 13 and 17 can build on the completed Focus Group on Quantum Information Technology for Networks, which developed terminology, use cases, and a standardization outlook (ITU-T, 2021). IEEE initiatives can complement these processes with performance, software, and engineering

CC BY

standards. Participation rules should include public laboratories, firms, universities, and users from countries without large domestic quantum programs so that standards do not simply codify the preferences of the most powerful ecosystems.

Second, post-quantum cryptography requires coordinated implementation rather than another declaration of principles. NIST's FIPS standards provide concrete technical baselines, but migration depends on national inventories, procurement rules, vendor testing, workforce capacity, and deadlines. Governments should publish sector-specific transition milestones, require cryptographic agility in public procurement, and establish interoperable validation and incident-reporting procedures. Mutual recognition can reduce duplication without obliging every jurisdiction to adopt identical risk tolerances. The priority is measurable migration progress, especially in high-value and long-lived systems.

Third, anticipatory governance should be institutionalized through recurring horizon scanning, risk registers, and stakeholder review. The OECD Framework for Anticipatory Governance of Emerging Technologies identifies anticipation, inclusion, adaptivity, and international cooperation as capabilities that can be embedded before risks harden into path dependence (OECD, 2024). The OECD Global Forum on Technology already provides a venue for dialogue on quantum policy among members, non-members, industry, researchers, labor, and civil society. It could host a periodic quantum governance review that compares strategies, access, workforce, security measures, and distributional effects without disclosing sensitive technical information. Fourth, confidence-building measures should distinguish legitimate security from performative secrecy. Governments can share non-sensitive benchmark definitions, disclose public funding categories, report safety or cybersecurity incidents, and publish aggregate information on access to public infrastructure. Research-security rules should be specific, reviewable, and proportionate, preserving international scientific collaboration where risks can be managed. These measures would not eliminate strategic rivalry, but they could reduce misperception, improve evidence quality, and make the governance of dual-use capabilities more accountable. Together, the four mechanisms connect institutional reality to the three vertices of the triangle: public authorities set obligations, markets implement and innovate, and standards bodies stabilize expectations.

Distributional governance is a fifth, cross-cutting requirement. Publicly financed infrastructure should publish transparent eligibility criteria and report the sectoral, geographic, and institutional distribution of access. Workforce programs should extend beyond elite physics and computer-science centers to include engineering, cybersecurity, law, ethics, public administration, and technical education. International capacity-building should enable less-resourced countries to participate in standards discussions and cryptographic migration rather than leaving them to adopt systems designed elsewhere. Democratization does not mean unrestricted access to sensitive capability; it means that exclusions, priorities, and public benefits are reasoned, reviewable, and proportionate (Seskir et al., 2023).

LIMITATIONS AND FUTURE RESEARCH

The analysis has five limitations. First, it relies on publicly available documents and therefore inherits substantial asymmetries in disclosure, especially for security-linked Chinese programs. Because the China corpus relied primarily on official English-language portals, it may

CC BY

privilege centrally authorized policy framings and underrepresent subnational implementation, domestic scholarly debate, negative results, and contested evidence. This asymmetry can bias the China case toward formal strategic intent more than the U.S. and EU cases, for which a wider and more granular documentary record is available; cross-case claims about transparency and implementation are therefore interpreted more cautiously for China.

Second, policy commitments are not equivalent to implementation, and the study does not normalize budgets, procurement, patents, or machine performance across jurisdictions. Third, the cases are internally heterogeneous: U.S. agencies, Chinese localities, EU institutions, and member states may pursue divergent priorities. Fourth, the observation window captures a rapidly changing field, so the position of each case within the triangle should be treated as time-bound. Fifth, the strategic triangle necessarily simplifies interactions among science, finance, defense, education, and civil society. Future research should test the framework with multilingual document corpora, comparable budget and patent data, infrastructure-access statistics, network analysis of standards participation, and interviews with policymakers, scientists, firms, and civil-society organizations. Longitudinal studies could then assess whether shifts in institutional configuration predict commercialization, interoperability, cryptographic readiness, or broader access.

CONCLUSION

This article has asked how the distribution of steering capacity among public institutions, market actors, and normative or standard-setting bodies shapes quantum governance in China, the United States, and the European Union. The comparison shows that national labels conceal hybrid institutional configurations. China's advantage lies in concentrated state direction and continuity; the United States combines decentralized market experimentation with substantial federal missions and technical standard-setting; and the EU joins multilevel public investment to normative coordination while seeking greater industrial scale. These differences are not merely descriptive. They operate through identifiable mechanisms that affect resource mobilization, commercialization, transparency, interoperability, and access.

The strategic triangle makes this argument operational. State, market, and norms are treated as comparable dimensions with explicit indicators, not as metaphors or mutually exclusive regime types. Applied consistently, the framework reveals both divergence and convergence. The cases retain distinct allocations of authority, yet all three are increasing public coordination, connecting quantum policy to security, and competing over standards. The most important finding is therefore that quantum power is institutional: technological capability depends on the arrangements that fund it, validate it, commercialize it, secure it, and render it interoperable.

This conclusion also tempers claims of imminent geopolitical rupture. Large-scale quantum computing may create significant advantages in selected domains, but present policy should be based on uncertainty, staged evidence, and the long implementation timelines of critical infrastructure. The immediate governance tasks are concrete: cryptographic migration, credible benchmarks, shared terminology, infrastructure access, workforce development, and proportionate research security. Treating future capabilities as already realized can distort priorities and intensify rivalry without improving preparedness.

CC BY

International governance should consequently be built as a layered system rather than as an unattainable comprehensive treaty. ISO/IEC, ITU-T, IEEE, NIST-linked technical processes, the OECD Global Forum on Technology, national authorities, and regional institutions can perform complementary functions if their responsibilities and interfaces are explicit. Such an architecture would not dissolve competition, but it could channel competition toward interoperable, auditable, and more responsible development. The broader contribution of the comparison is to show that the future quantum order will be shaped not only by who achieves a technical breakthrough, but by which institutions can convert uncertainty into legitimate and durable coordination.

CC BY

CRediT AUTHOR STATEMENT

Daniele Battista: Conceptualization; Methodology; Investigation; Formal analysis; Writing – original draft; Writing – review & editing; Visualization; Project administration. **Arthur Amadeus Salvatore Gugliucciello:** Conceptualization; Methodology; Investigation. **Alessandra Petrone:** Supervision; Writing – review & editing.

All authors have read and agreed to the published version of the article.

COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments:
Not applicable.

Funding:
Not applicable.

AI Declaration:
The authors acknowledge the use of ChatGPT (OpenAI) to assist with English-language editing and the clarity of selected passages during revision. The tool was used solely for language refinement and was not treated as a source or used to generate empirical evidence. All arguments, evidence, citations, and factual claims were independently verified by the authors, who assume full responsibility for the manuscript's originality, accuracy, validity, and integrity.

Statement of Human Rights:
This article does not contain any studies involving human participants performed by any of the authors.

Informed Consent:
Not applicable.

Disclosure statement:
To maintain transparency and integrity, Dr. Daniele Battista, a member of the journal's auxiliary committee, has recused himself from all editorial decisions concerning this article. All editorial responsibilities for the article were carried out independently by other editorial board members. The co-authors have declared no conflicts of interest.

PUBLISHER'S NOTE

Neutrality Statement on Jurisdictional Claims and Institutional Affiliations:

The publisher and the journal remain neutral regarding jurisdictional claims in published maps and institutional affiliations.

Language Quality and Author Responsibility Policy:

The publisher and the journal use AI-assistive tools to enhance the language quality of accepted articles. These tools help refine grammar, clarity, and readability while preserving the integrity of the original text. However, authors retain full responsibility for the accuracy and content of their work.

Disclaimer on External Links:

The publisher and the journal cannot be held responsible for the content of external websites or any broken or missing links within the article. Authors are solely responsible for ensuring the accuracy and functionality of all hyperlinks at the time of submission.

REFERENCES

1. Aboy, Mateo, Urs Gasser, I. Glenn Cohen, and Mauritz Kop. 2025. "Quantum Technology Governance: A Standards-First Approach." *Science* 389 (6760): 575–578. https://doi.org/10.1126/science.adw0018.
2. Arthur, W. Brian. 1989. "Competing Technologies, Increasing Returns, and Lock-In by Historical Events." *Economic Journal* 99 (394): 116–131. https://doi.org/10.2307/2234208.
3. Atladottir, Drifa, Neele Roch, Matthias Leese, and Verena Zimmermann. 2025. "A Quantum of Responsibility? A Comparison of National Quantum Governance Frameworks and Expert Views." *Digital Society* 4 (2): 54. https://doi.org/10.1007/s44206-025-00205-7.
4. Battista, Daniele. 2024. "Political Communication in the Age of Artificial Intelligence: An Overview of Deepfakes and Their Implications." *Society Register* 8 (2): 7–24. https://doi.org/10.14746/sr.2024.8.2.01.
5. Battista, Daniele, and Emiliana Mangone. 2025. "Technological Culture and Politics: Artificial Intelligence as the New Frontier of Political Communication." *Societies* 15 (4): 75. https://doi.org/10.3390/soc15040075.
6. Coenen, Christopher, Alexei Grinbaum, Armin Grunwald, Colin Milburn, and Pieter E. Vermaas. 2022. "Quantum Technologies and Society: Towards a Different Spin." *NanoEthics* 16 (1): 1–6. https://doi.org/10.1007/s11569-021-00409-4.
7. Edler, Jakob, and Jan Fagerberg. 2017. "Innovation Policy: What, Why, and How." *Oxford Review of Economic Policy* 33 (1): 2–23. https://doi.org/10.1093/oxrep/grx001.
8. EPO/OECD. 2025. *Mapping the Global Quantum Ecosystem: A Comprehensive Analysis Based on Innovation, Firm, Investment, Skills, Trade and Policy Data*. Munich and Paris: European Patent Office and OECD Publishing. https://doi.org/10.65216/20251217-0001.
9. EuroHPC Joint Undertaking. 2026. "Inauguration of SOL, a New Quantum Computer Together with the LISA Upgrade of the LEONARDO Supercomputer." 11 June, 2026. https://www.eurohpc-ju.europa.eu/inauguration-sol-new-quantum-computer-together-lisa-upgrade-leonardo-supercomputer-2026-06-11_en.
10. European Commission. 2025. *Quantum Europe Strategy*. COM(2025) 363 final, 2 July, 2025. https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy.
11. Farrell, Henry, and Abraham L. Newman. 2019. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44 (1): 42–79. https://doi.org/10.1162/isec_a_00351.
12. George, Alexander L., and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.
13. Hoofnagle, Chris Jay, and Simson L. Garfinkel. 2022. *Law and Policy for the Quantum Age*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108911511.
14. Hughes, Thomas P. 1987. "The Evolution of Large Technological Systems." In *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, edited by Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, 51–82. Cambridge, MA: MIT Press.
15. ISO/IEC. 2024. "JTC 3: Quantum Technologies." Accessed 16 August, 2026. https://www.iso.org/committee/10138914.html.

16. ITU-T. 2021. *Standardization Outlook and Technology Maturity: Network Aspects of Quantum Information Technologies*. Focus Group on Quantum Information Technology for Networks, Deliverable D1.4. Accessed 16 August, 2026. https://www.itu.int/pub/T-FG-QIT4N-2021-D1.4.
17. Kim, Mi-jin, Heejin Lee, and Jooyoung Kwak. 2020. "The Changing Patterns of China's International Standardization in ICT under Techno-Nationalism: A Reflection through 5G Standardization." *International Journal of Information Management* 54: 102145. https://doi.org/10.1016/j.ijinfomgt.2020.102145.
18. Mann, Michael. 1984. "The Autonomous Power of the State: Its Origins, Mechanisms and Results." *European Journal of Sociology* 25 (2): 185–213. https://doi.org/10.1017/S0003975600004239.
19. Manners, Ian. 2002. "Normative Power Europe: A Contradiction in Terms?" *Journal of Common Market Studies* 40 (2): 235–258. https://doi.org/10.1111/1468-5965.00353.
20. Mazzucato, Mariana, and Gregor Semieniuk. 2017. "Public Financing of Innovation: New Questions." *Oxford Review of Economic Policy* 33 (1): 24–48. https://doi.org/10.1093/oxrep/grw036.
21. Molas-Gallart, Jordi. 1997. "Which Way to Go? Defence Technology and the Diversity of Dual-Use Technology Transfer." *Research Policy* 26 (3): 367–385. https://doi.org/10.1016/S0048-7333(97)00023-1.
22. Mosca, Michele. 2018. "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *IEEE Security & Privacy* 16 (5): 38–41. https://doi.org/10.1109/MSP.2018.3761723.
23. NIST (National Institute of Standards and Technology). 2024a. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. FIPS 203. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.FIPS.203.
24. NIST (National Institute of Standards and Technology). 2024b. *Module-Lattice-Based Digital Signature Standard*. FIPS 204. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.FIPS.204.
25. NIST (National Institute of Standards and Technology). 2024c. *Stateless Hash-Based Digital Signature Standard*. FIPS 205. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.FIPS.205.
26. NQIAC (National Quantum Initiative Advisory Committee). 2024. *Quantum Networking: Findings and Recommendations for Growing American Leadership*. Washington, DC: Office of Science and Technology Policy. Accessed 16 August, 2026. https://www.quantum.gov/wp-content/uploads/2024/09/NQIAC-Quantum-Networking-Report.pdf.
27. NSTC (National Science and Technology Council). 2024. *National Quantum Initiative Supplement to the President's FY 2025 Budget*. Washington, DC: Executive Office of the President. Accessed 16 August, 2026. https://www.quantum.gov/wp-content/uploads/2024/12/NQI-Annual-Report-FY2025.pdf.
28. OECD. 2024. *Framework for Anticipatory Governance of Emerging Technologies*. OECD Science, Technology and Industry Policy Papers, no. 165. Paris: OECD Publishing. https://doi.org/10.1787/0248ead5-en.

29. OECD. 2025a. *A Quantum Technologies Policy Primer*. OECD Digital Economy Papers, no. 371. Paris: OECD Publishing. https://doi.org/10.1787/fd1153c3-en.
30. OECD. 2025b. *An Overview of National Strategies and Policies for Quantum Technologies*. OECD Digital Economy Papers, no. 379. Paris: OECD Publishing. https://doi.org/10.1787/5e55e7ab-en.
31. Perrier, Elija. 2022. "The Quantum Governance Stack: Models of Governance for Quantum Information Technologies." *Digital Society* 1 (3): 22. https://doi.org/10.1007/s44206-022-00019-x.
32. Radu, Roxana. 2019. *Negotiating Internet Governance*. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780198833079.001.0001.
33. Seskir, Zeki C., Steven Umbrello, Christopher Coenen, and Pieter E. Vermaas. 2023. "Democratization of Quantum Technologies." *Quantum Science and Technology* 8 (2): 024005. https://doi.org/1088/2058-9565/acb6ae.
34. State Council of the People's Republic of China. 2021. *Outline of the 14th Five-Year Plan (2021–2025) for National Economic and Social Development and the Long-Range Objectives through the Year 2035*. Accessed 16 August, 2026. https://wb.fujian.gov.cn/English/usefulinformation/NewInitiatives/202108/t20210809_5666236.htm.
35. Ten Holter, Carolyn, Philip Inglesant, and Marina Jirotka. 2023. "Reading the Road: Challenges and Opportunities on the Path to Responsible Innovation in Quantum Computing." *Technology Analysis & Strategic Management* 35 (7): 844–856. https://doi.org/10.1080/09537325.2021.1988070.
36. United States Congress. 2018. *National Quantum Initiative Act*. Public Law 115-368, 132 Stat. 5092. Accessed 16 August, 2026. https://www.congress.gov/115/plaws/publ368/PLAW-115publ368.pdf.
37. White House, The. 2026a. "Securing the Nation Against Advanced Cryptographic Attacks." Executive Order 14412, 22 June, 2026. *Federal Register* 91: 38483–38486. https://www.federalregister.gov/documents/2026/06/25/2026-12909/securing-the-nation-against-advanced-cryptographic-attacks.
38. White House, The. 2026b. "Ushering in the Next Frontier of Quantum Innovation." Executive Order 14413, 22 June, 2026. *Federal Register* 91: 38487–38491. https://www.federalregister.gov/documents/2026/06/25/2026-12910/ushering-in-the-next-frontier-of-quantum-innovation.
39. Zuniga, Nicolas, Saheli D. Burton, Filippo Blancato, and Madeline Carr. 2024. "The Geopolitics of Technology Standards: Historical Context for US, EU and Chinese Approaches." *International Affairs* 100 (4): 1635–1652. https://doi.org/10.1093/ia/iiae102.