GLOBAL QUANTUM LAW: PHYSICS, CAPITALISM, AND INFRASTRUCTURE

MARCO GERMANÒ*

This commentary argues that the development of quantum computing demands a regulatory approach grounded in its infrastructural dimensions, which shape access, control, and participation globally, rather than in abstract ethical guidance alone. Introducing the concept of global quantum law, it contends that early decisions about system design and deployment are already forming the basis of a transnational legal regime that connects engineering architectures with emerging governance frameworks. By examining pressing challenges such as encryption standards, intellectual property, and the risk of monopolization, the piece highlights how quantum computing's promise is unfolding within a deeply unequal global landscape. The core question it poses is whether current governance efforts can prevent the concentration of quantum power in the hands of a few or whether they risk reproducing the exclusions of previous technological revolutions.

[*] LL.M. Candidate in International Legal Studies, New York University (NYU) School of Law. Graduate Editor, N.Y.U. Journal of International Law & Politics. Research Assistant at Guarini Global Law & Tech (GGLT), NYU. Student Fellow at the Privacy Research Group (PRG), NYU. I am grateful to Professor Benedict Kingsbury for his thoughtful comments on earlier drafts. I am also grateful for the JILP editorial team, particularly Marianna Troia and Oscar Miller, for their editorial work. All views expressed are my own and do not necessarily reflect those of any affiliated institution. Any remaining errors are mine alone.

I. INTRODUCTION

Over thirty years ago, physicist John Preskill famously posed two questions about quantum computing: whether we truly wanted to build these machines, and whether we even could.[1] Both questions have since been answered with a resounding yes. Around the globe, government agencies, major corporations, and academic institutions have been channeling significant resources into moving quantum computers from theory to practice.[2] Once considered purely speculative, this field is now widely viewed as a transformative force that will reshape technological innovation and influence major aspects of our digital economy, with associated impacts on international governance frameworks.[3]

Today, the question is no longer whether to develop quantum computing, but how to best guide its progress.[4] Against this backdrop, a broad set of stakeholders has begun to scrutinize the regulatory consequences of this emerging technology.[5] In legal circles, there is growing debate over the need for a legal framework that remains attentive to the unique features and complexities arising from quantum mechanics and its application in

[1] *See* John Preskill, *Quantum Computing: Pro and Con*, 454 PROC. ROYAL SOC'Y LONDON A 469, 469 (1998) (assessing the potential of quantum computation).

[2] Sylvain Duranton, *Quantum Computing Takes Off With $55 Billion in Global Investments*, FORBES (June 26, 2024), https://www.forbes.com/sites/sylvainduranton/2024/06/26/quantum-now/.

[3] *See, e.g.*, CAROLYN TEN HOLTER ET AL., CREATING A RESPONSIBLE QUANTUM FUTURE: THE CASE FOR A DEDICATED NATIONAL RESOURCE FOR RESPONSIBLE QUANTUM COMPUTING (Oxford Responsible Technology Institute 2021), https://www.rti.ox.ac.uk/wp-content/uploads/2022/09/Ten_Holter_et_al_2021_creating_a_responsible.pdf (discussing societal implications of quantum computing development and arguing for a "responsible innovation" approach to govern this technology); Kasim Balarabe, *Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap*, EUR. J. RISK REGUL., 2025, at 1–20 (highlighting intellectual property, data security, regulation, and ethical challenges emerging from quantum computing).

[4] *See generally* Aurelija Lukoseviciene, *Regulating Quantum Computers: Insights into Early Patterns and Trends in Academic Regulatory Conversations on the 'Quantum Revolution'*, 17 L., INNOVATION & TECH. 241 (2025) (identifying the current questions in academic conversations about regulating quantum technology).

[5] *See generally* CHRIS JAY HOOFNAGLE & SIMSON L. GARFINKEL, LAW AND POLICY FOR THE QUANTUM AGE (Cambridge Univ. Press 2022) (providing an overview of how the policy landscape in the United States and other liberal democracies should respond to the opportunities and challenges brought on by quantum information science).

computing—an area some have begun calling *quantum law*.[6] Although the contours of this field remain somewhat undefined, it has sparked lively debates, ranging from the design of technology-specific regulations to guide the ethical development of quantum technology to propositions of radical reimaginations of legal doctrines adapted to quantum mechanics.[7]

This commentary approaches these conversations from a different angle. It argues that the political and economic development of quantum computing will likely depend less on legal-ethical frameworks and more on the governing of its infrastructural dimensions.[8] In fact, recognizing this from the outset of regulatory discussions is important to avoid repeating the shortcomings of past governance efforts related to recent technological shifts, such as the internet and digital platforms, where some approaches prioritized poorly targeted regulatory goals, while others paved the way for monopolistic power structures in the digital sphere.[9]

This commentary proceeds in four parts, followed by a conclusion. Part II outlines the fundamentals of quantum computing and begins to unpack its infrastructural dimensions. Part III examines key international governance issues arising from quantum computing, focusing on cybersecurity and geopolitics, intellectual property (IP) and innovation, and infrastructural gatekeeping and emerging monopolies. Part IV introduces what this commentary terms *global quantum law*—the ways in which emerging legal frameworks extend beyond national jurisdictions, drawing on a mix of

[6] *See, e.g.,* Elizaveta A. Gromova & Sergey A. Petrenko, *Quantum Law: The Beginning*, 1 J. DIG. TECH. & L. 62, 69–82 (2023) (exploring quantum law as the law of the future due to the distinctive properties of quantum phenomena and the regulatory challenges posed by emerging quantum technologies). *See also* THE QUANTUM LAW PROJECT, http://quantum-law.org/ (showcasing the Lund University Faculty of Law project dedicated to the study of the legal implications of quantum computing) (last visited Apr. 12, 2025).

[7] *See, e.g.*, Mauritz Kop, *Establishing a Legal-Ethical Framework for Quantum Technology,* YALE J. L. & TECH. BLOG (Mar. 30, 2021), https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology (discussing designing a culturally sensitive legal-ethical framework for applied quantum technologies) (last visited Mar. 9, 2025); Jeffrey Ritter, *Digital Justice in 2058: Trusting Our Survival to AI, Quantum and the Rule of Law*, 8 J. INT'L & COMPAR. L. 333, 335 (2021) (arguing that quantum law invites a complete re-imagining of legal systems rooted in quantum mechanics rather than in traditional human-centered rules).

[8] *See* Benedict Kingsbury, *Infrastructure and InfraReg: On Rousing the International Law 'Wizards of Is'*, 8(2) CAMBRIDGE INT'L L. J. 171, 177 (2019) (putting forward the idea of "infrastructure as regulation" as a way of "opening up thinking about international law and technology of all kinds.").

[9] *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 15–47 (Oxford Univ. Press 2019) (exploring how regulatory choices around recent digital transformations in information capitalism have enabled the emergence of monopolistic power structures, particularly in data control.)

transnational legal technologies and technical standardization efforts to govern the development of *quantum infrastructures*.[10] Part V brings together the previous analyses to argue that current governance frameworks risk reinforcing the power imbalances that accompanied earlier technological transitions. This commentary thus concludes by suggesting that, much like *qubits* (quantum bits) can exhibit unpredictable behavior, the trajectory of quantum technology remains uncertain. The urgent task is to discuss and design effective governance strategies that safeguard quantum computing's promise while mitigating the risk of deepening societal inequities.[11]

II. QUANTUM COMPUTING 101

Quantum computing represents a striking departure from the classical physics that has shaped digital technology since the 1960s.[12] Early computers from that era—and those we use now—operate through an architecture encoding information in *bits* (0s or 1s). These devices, linked via undersea cables, radio waves, satellite links, among other means, can exchange any type of information, from simple text messages to complex data streams (e.g., videos, real-time sensor data, or massive scientific datasets). This simple yet powerful design underpins many technologies ranging from smartphones to global communication networks. However, it also reveals a key limitation: even as processing speeds increase, each computational step must be completed sequentially, imposing inherent constraints.

[10] By "quantum infrastructures", this commentary refers to the interconnected social, technical, and political systems required for quantum computing. They encompass specialized hardware (e.g., cryogenic systems and qubits), software stacks for quantum control and algorithm design, supply chains for critical materials, regulatory and funding mechanisms, error-correction protocols, and other coordinating frameworks that collectively enable the development and use of quantum technologies at scale. *Thinking infrastructurally* about quantum thus also requires attention to the institutions and processes that govern these systems—including standard-setting bodies, certification regimes, government procurement agencies, and self-regulatory organizations—that translate technical specifications into enforceable norms, shape market access, and distribute expertise and authority. *See* Angelina Fisher & Thomas Streinz, *Confronting Data Inequality*, 60 COLUM. J. TRANSNAT'L L. 829, 852 (using a similar analytical approach to data infrastructures).

[11] *See, e.g.*, PIETER VERMAAS & ULRICH MANS, QUANTUM TECHNOLOGIES AND THEIR GLOBAL IMPACT: DISCUSSION PAPER 9–15 (UNESCO & Quantum Delta 2024) (discussing possible pathways to develop quantum technologies for the public good.).

[12] *See generally* MICHAEL A. NIELSEN & ISAAC L. CHUANG, QUANTUM COMPUTATION AND QUANTUM INFORMATION 1–13 (10th Anniversary ed., Cambridge Univ. Press 2010); CHRIS BERNHARDT, QUANTUM COMPUTING FOR EVERYONE 171–189 (MIT Press 2019).

By contrast, quantum computers operate using *qubits*, which differ from traditional bits in three fundamental ways. First, qubits can represent multiple values at once—a phenomenon called *superposition*, where information is encoded as both 0 and 1 until measured. Second, qubits can be used in algorithmic designs to harness superposition in a way that highlights promising "solutions" while downplaying less effective ones—an interference-based technique known as *amplitude amplification* that accelerates complex computations. Third, qubits can remain interconnected so that measuring one instantly influences the others, no matter how far apart they are—a property known as *entanglement*, where correlated qubits share a unified quantum state. Taken together, these qubits characteristics promise transformative advances in processing power, encryption, and simulation, enabling quantum computers to tackle challenges beyond the reach of classical machines.

A helpful way to see these transformative differences is through analogy. In a traditional device, exchanging information is like mailing letters (bits) one by one; the recipient assembles them into words, sentences, and ultimately a complete message. In a radically different approach, quantum computing is as though all possible versions of that message are sent at once, with quantum interference used to amplify the most promising outcomes—so that when the message is finally opened and read (i.e., measured), the correct version is far more likely to appear. For a practical real-world illustration, consider drug discovery for a complex disease. Traditionally, researchers test one molecular configuration at a time, much like trying different letters in a word until they find the one that "fits" the disease target. A quantum computer, on the other hand, can explore many configurations in parallel, rapidly zeroing in on promising solutions. This leap can significantly reduce the time from initial screening to viable treatment.

Though the underlying physics may seem intricate, quantum computing's potential extends well beyond theory. Existing prototypes have already accomplished tasks that challenge conventional supercomputers, pointing toward substantial future applications in quantum sensing, cryptanalysis, next-generation AI, and internet communication.[13] In fact, the

[13] Existing prototypes have already accomplished tasks that challenge conventional supercomputers. In one widely discussed experiment, a superconducting processor executed a random circuit sampling task in a few minutes that was estimated to take classical systems thousands of years—though subsequent analysis questioned the practical relevance of the benchmark. More recently, research teams have reported achieving over 100 physical qubits with exponential error suppression, and experimental architectures using topological or "cat" qubits have shown promise in reducing error rates through hardware-level innovations. Other groups working on quantum annealing have demonstrated speedups for specific problems, such as materials simulation, that would be intractable for classical machines. These breakthroughs fuel

range of potential applications is vast and still not fully mapped.[14] Yet these possibilities face significant implementation hurdles. Notably, qubits are highly sensitive to external noise and often require cryogenic temperatures and specialized shielding techniques to preserve their fragile quantum state (known as *coherence*).[15] Significant fabrication costs, a still-nascent skilled workforce, supply chain complexities, and energy and environmental concerns likewise constrain scalability and large-scale implementation.[16] Furthermore, the progress of quantum computing remains uneven and sector-specific. Some applications, especially those involving noisy intermediate-scale quantum (NISQ) devices, face mathematical challenges.[17] Others, particularly outside military and pharmaceutical sectors, may never justify the high costs of implementation.[18] The promise of disruption is thus real,

considerable enthusiasm, but most remain still confined to narrow domains or hardware-specific advantages. For additional background, see Frank Arute et al., *Quantum Supremacy Using a Programmable Superconducting Processor*, 574 NATURE 505, 505–510 (2019); Catherine Bolgar, *Microsoft's Majorana 1 Chip Carves New Path for Quantum Computing*, MICROSOFT SOURCE (Feb. 19, 2025), https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/; Michael Newman & Kevin Satzinger, *Making Quantum Error Correction Work*, GOOGLE RESEARCH (Dec. 9, 2024), https://research.google/blog/making-quantum-error-correction-work/; Fernando Brandão & Oskar Painter, *Amazon Announces Ocelot Quantum Chip,* AMAZON SCIENCE (Feb. 27, 2025), https://www.amazon.science/blog/amazon-announces-ocelot-quantum-chip; Matt Swayne, *D-Wave Deep Dive: A Look at the Quantum Advantage Findings—And The Questions That Remain,* QUANTUM INSIDER (Mar. 13, 2025), https://thequantuminsider.com/2025/03/13/d-wave-deep-dive-a-look-at-the-quantum-advantage-findings-and-the-questions-that-remain/.

[14] *See generally* Stephanie Wehner, David Elkouss, & Ronald Hanson, *Quantum Internet: A Vision for the Road Ahead*, 362 SCIENCE eaam9288 (2018) (proposing that quantum technology could be used to develop a new internet architecture and would reduce latency to near-instant communication).

[15] Coherence refers to the ability of a qubit to maintain its quantum state over time. This delicate state is easily disrupted by interactions with the surrounding environment, such as electromagnetic interference or thermal vibrations, which introduce noise and cause decoherence. To minimize these effects, quantum systems are typically operated at cryogenic temperatures and isolated using shielding techniques to prolong coherence times and ensure reliable computation. For additional background, see *supra* note 14.

[16] Jian-Wei Pan, *Quantum Technologies Need Big Investments to Deliver on Their Big Promises*, NATURE (Feb. 26, 2025), https://www.nature.com/articles/d41586-025-00564-8.

[17] *See* Nat Rubio-Licht, *The Costs and Benefits of Quantum Computing,* THE DAILY UPSIDE (Dec. 8, 2024) (noting the currently very hard limits to the stabilization of a qubit: "And to solve major computation problems, these devices will need 'another two to three to 10 to 100 times more qubits'.") https://www.thedailyupside.com/technology/the-costs-and-benefits-of-quantum-computing/.

[18] *See* Michael Bogobowicz et al., *Steady progress in approaching the quantum advantage*, MCKINSEY DIGITAL (Apr. 24, 2024) (opining that "four sectors—chemicals,

but not universal. Treating quantum as a general-purpose technology may obscure the infrastructural and political contingencies that determine where and for whom it will truly matter.

These challenges underscore a key aspect of the *second* quantum revolution:[19] quantum computers rely not just on advances in hardware or software but also on robust technical, social, political, and organizational systems—in other words, *quantum infrastructures*.[20] These infrastructures are not neutral or merely technical backdrops; they are actively governed through decisions about how systems are deployed, who sets design standards, and what forms of compliance and certification are required. Deployment design standards, for example, determine which hardware architectures become dominant, which interoperability features are prioritized, and what levels of error correction are acceptable for operational use. These decisions, which have implications for who gets to access and benefit from such technology, are typically negotiated in closed or semi-closed settings involving industry consortia, standards development organizations (SDOs), and national regulators. While these actors may formally codify technical norms, market dynamics and informal negotiations among industry players also shape outcomes, often reinforcing the preferences of the most resource-rich or strategically positioned firms.[21]

At stake in these processes is not only functionality but also legitimacy: infrastructures gain legal and economic traction when they are certified as conforming to *best practices* or technical norms, which in turn reflect specific assumptions about risk, security, and value. As a result, governance becomes embedded in infrastructure, not as an add-on, but as an intrinsic part of quantum systems. This interplay of hardware, logistics,

life sciences, finance, and mobility—are likely to see the earliest impact from quantum computing . . . .") https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage.

[19] The so-called "first quantum revolution" refers to technologies developed in the 20th century—such as semiconductors, lasers, and MRI—that rely on quantum mechanics to explain underlying physical behavior but operate in predictable, classical ways. These technologies do not manipulate quantum states directly during use. In contrast, the "second quantum revolution" involves the deliberate control of quantum states (such as superposition and entanglement) as active resources for computation, communication, and sensing. This allows quantum systems to outperform classical ones in specific tasks, enabling exponential gains in computing power, provably secure cryptographic protocols, and ultra-sensitive measurement techniques. Jonathan P. Dowling & Gerard J. Milburn, *Quantum Technology: The Second Quantum Revolution*, 361 PHIL. TRANSACTIONS ROYAL SOC'Y A 1655, 1655–1656 (2003).

[20] *See supra* note 11.

[21] JUSTUS BARON ET AL., MAKING THE RULES: THE GOVERNANCE OF STANDARD DEVELOPMENT ORGANIZATIONS AND THEIR POLICIES ON INTELLECTUAL PROPERTY RIGHTS (JRC Science for Policy Report 2019), https://ssrn.com/abstract=3364722.

and power creates a complex global landscape for the governance of quantum computing.

III. INTERNATIONAL GOVERNANCE CHALLENGES

Quantum computing introduces governance questions that go well beyond technical specifications, touching on legal, geopolitical, and infrastructural concerns. As emerging technologies present both opportunities and systemic hurdles, effective governance will require regulatory strategies attuned to quantum's distinctive features, while also building on lessons from past digital transformations. Although this commentary does not offer an exhaustive review of these complexities, the next section outlines three policy domains currently drawing international attention in quantum governance: (i) cybersecurity and geopolitics, (ii) IP and innovation, and (iii) infrastructural gatekeeping and emerging monopolies. Each area illustrates how advances in quantum computing can produce ripple effects across regulatory and societal frameworks. I briefly examine each before turning to an analysis of the strengths and gaps in current governance approaches.

First, one of the chief concerns about quantum computing is its potential to undermine the cryptographic architecture that safeguards much of our digital world. Encryption lies at the heart of modern data security, transforming readable plaintext into unreadable ciphertext using mathematical algorithms.[22] It underpins everything from financial transactions and personal communications to cloud storage, relying on computationally difficult problems—such as factoring large prime numbers—that conventional computers cannot solve efficiently. Techniques such as end-to-end encryption (E2EE) further bolster these defenses by ensuring that only the sender and recipient can decrypt messages, blocking even the service provider from viewing the content.[23] To guide the development and ensure global application of encryption technologies, SDOs—like the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and the Internet Engineering Task Force (IETF)—define and maintain robust encryption practices, such as the RSA

[22] *See* Charles Duan & James Grimmelmann, *Content Moderation on End-to-End Encrypted Systems: A Legal Analysis*, 8 GEO. L. TECH. REV. 1, 9–17 (2024) (providing an overview of encryption and how it is intertwined with national security).

[23] Kaspersky Team, *What End-to-End Encryption Is, and Why You Need It*, KASPERSKY DAILY (Sept. 11, 2020), https://usa.kaspersky.com/blog/what-is-end-to-end-encryption/23288/.

standard,[24] a widely used public-key cryptosystem for secure data transmission.[25] This framework has proven effective in protecting digital communications worldwide over the last decades, ensuring safety and interoperability.

Quantum computing, however, complicates this landscape.[26] If a cryptographically relevant quantum computer emerges, widely used methods such as RSA could become instantly vulnerable to rapid decryption, potentially exposing enormous amounts of previously protected data.[27] As a result, global stakeholders have begun warning of the seismic geopolitical implications quantum technologies could have if one actor achieves quantum-based codebreaking or secure communications before others.[28] Indeed,

[24] R. L. Rivest, A. Shamir, & L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 21 Commc'n ACM 120 (1978)

[25] *See, e.g.,* Nat'l Inst. of Standards & Tech., NIST Special Publication 800-78-5 (Initial Public Draft), Cryptographic Algorithms and Key Sizes for Personal Identity Verification (Apr. 2024), https://csrc.nist.gov/pubs/sp/800/78/5/ipd (last visited May 13, 2025); ISO/IEC 9796 RSA Digital Signature Schemes, https://www.cryptsoft.com/pkcs11doc/v220/group__SEC__12__1__11__ISO__IEC__9796__RSA.html (last visited May 13, 2025).; RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2 (Int'l Eng'g Task Force Nov. 2016), https://datatracker.ietf.org/doc/html/rfc8017.

[26] *See* Michele Mosca, *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?*, 16(5) IEEE Sec. & Priv. Mag. 38, 38–41 (2018); John Preskill, *Quantum Computing in the NISQ Era and Beyond*, 2 Quantum 79 (2018); Emerging Tech. from the arXiv, *How a Quantum Computer Could Break 2048-Bit RSA Encryption in 8 Hours*, MIT Tech. Rev. (May 30, 2019), https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.

[27] A widely cited example of quantum computing's disruptive potential is Shor's algorithm, which could, in principle, break widely used encryption methods like RSA by factoring large numbers far more efficiently than classical computers. Another example, Grover's algorithm, could speed up search processes that underlie many security and data applications. While these algorithms are theoretical for now, they illustrate the stakes: if large-scale, fault-tolerant quantum computers become viable, core elements of today's digital infrastructure—especially encryption—could be compromised. Realizing this potential, however, still depends on substantial advances in quantum hardware and error correction. Peter W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, *in* Proceedings of the 35th Annual Symposium on Foundations of Computer Science 124 (IEEE Press ed., 1994); Lov K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, *in* Proceedings of the 28th Annual ACM Symposium on Theory of Computing 212 (1996). *See also* Ashley Montanaro, *Quantum Algorithms: An Overview*, 2 Npj Quantum Info. 1 (2016) (providing a nontechnical survey of major quantum algorithms and current hardware constraints).

[28] *See* Organization for Economic Co-operation and Development (OECD), *A Quantum Technologies Policy Primer* 42 (OECD Digital Economy Paper No. 371, 2025) (underscoring how "[g]eopolitical competition and security concerns over quantum

a breach of current cryptographic protocols could leave vital infrastructure vulnerable to sophisticated transnational cyberattacks.[29] Recognizing this threat, researchers and standards bodies have begun developing *post-quantum algorithms*—often built on structured lattices or hash-based schemes—aimed at resisting both classical and quantum attacks.[30] A handful of promising proposals have already been chosen for standardization, with others still under review.[31] Although these next-generation algorithms are expected to offer robust protection against quantum decryption methods, questions about their performance, interoperability, and broad adoption remain, especially as these techniques are relatively new and lack the decades of scrutiny that older cryptographic methods have.[32]

Second, the global patent and IP landscape surrounding quantum technology adds another layer of complexity in this second revolution.[33] Governments, defense contractors, and private corporations are investing vast resources into quantum R&D, striving to gain a competitive edge in areas such as secure communications, sensor technology, and advanced

technologies may result in more nationalised, closed ecosystems that are increasingly siloed in countries . . . .").

[29] Guilherme Schneider, *Quantum Computing and State-Sponsored Cyber Warfare: How Quantum Will Transform Nation-State Cyber Attacks*, MODERN DIPLOMACY (Nov. 7, 2024), https://moderndiplomacy.eu/2024/11/07/quantum-computing-and-state-sponsored-cyber-warfare-how-quantum-will-transform-nation-state-cyber-attacks/.

[30] Post-quantum algorithms are cryptographic methods designed to remain secure even against attackers equipped with quantum computers. Current widely used encryption systems, such as RSA and elliptic curve cryptography (ECC), depend on mathematical problems that quantum algorithms like Shor's could solve efficiently, making them vulnerable in a quantum future. In contrast, post-quantum cryptography relies on problems that are believed to be hard for both classical and quantum machines. Two of the most promising approaches are lattice-based and hash-based cryptography. Lattice-based methods use complex grid-like structures in many dimensions, where problems like finding the shortest path between points are computationally intense. Hash-based cryptography relies on one-way mathematical functions that convert any input into a scrambled output (a "hash") that is easy to verify but practically impossible to reverse. These approaches are being actively developed and standardized to ensure long-term data protection in a quantum-enabled world. *See supra* note 28.

[31] For background on ongoing standardization processes for post-quantum cryptography, see Federal Office for Information Security (BSI), *Post-Quantum Cryptography*, BSI, https://bit.ly/3FqoxLT (last visited Mar. 2, 2025); Nat'l Inst. of Standards & Tech. (NIST), *Post-Quantum Cryptography (PQC)*, NIST, https://csrc.nist.gov/projects/post-quantum-cryptography (last visited Mar. 9, 2025).

[32] *Limitations of Post-Quantum Cryptography*, ENCRYPTION CONSULTING, https://www.encryptionconsulting.com/education-center/limitations-of-post-quantum-cryptography/ (last visited Mar. 9, 2025).

[33] *See* Mauritz Kop, *Quantum Computing and Intellectual Property Law*, 36 BERKELEY TECH. L. J. 101, 102–115 (2021) (unpacking several IP challenges arising from quantum computing deployment.).

simulations.[34] Yet these rapid developments outpace existing IP frameworks, raising difficult questions about how to safeguard inventions that blend physics, engineering, and computer science in unprecedented ways. Quantum algorithms, for instance, can resemble mathematical formulas long treated as unpatentable subject matter, while new hardware breakthroughs often hinge on specialized materials and manufacturing techniques that do not fit neatly into classic IP categories.[35] This legal mismatch risks producing a patchwork of protections in which fundamental quantum knowledge is left exposed or, conversely, locked behind expansive trade secrets.

The stakes intensify in the defense sphere, where military applications and dual-use concerns intersect. In this context, national security restrictions—such as classification regimes and export controls—can severely limit who has access to emerging quantum technologies. These controls restrict academic and international collaboration, narrowing the pool of experts who can evaluate, critique, or improve quantum systems that may become critical to societal development. As strategic capabilities become siloed within military programs, states may reinforce competitive dynamics, fueling a new kind of arms race. The resulting secrecy and asymmetry risk entrenching long-term imbalances in global technological power, shaped not only by innovation itself but by the governance structures that determine who gets to use it.[36]

Indeed, quantum computing raises the prospect that a handful of corporations or nations could secure exclusive access to advanced quantum infrastructures. This leads to a third governance concern: the possibility that quantum development and deployment may result in global monopolies over the control of quantum infrastructure. Developing and operating fault-tolerant quantum machines demands extraordinary capital, deep specialized expertise, and highly complex manufacturing processes—all of which currently favor well-funded government labs and major tech firms.[37] Such

[34] Victoria Masterson, *Can we build a safe and inclusive 'quantum economy'?*, WORLD ECONOMIC FORUM (Feb. 5, 2024), https://www.weforum.org/stories/2024/02/quantum-economy-blueprint-world-economic-forum/.

[35] Mauritz Kop, Mateo Aboy, & Timo Minssen, *Intellectual Property in Quantum Computing and Market Power: A Theoretical Discussion and Empirical Analysis*, 17 J. INTELL. PROP. L. & PRAC. 613, 616–625 (2022).

[36] *See* David Lague, *U.S. and China Race to Shield Secrets from Quantum Computers*, REUTERS (Dec. 14, 2023), https://www.reuters.com/investigates/special-report/us-china-tech-quantum/ (arguing the United States and China are already engaged in what seems to be an IP race around quantum technology.)

[37] *See* OECD, *supra* note 30 at 49 ("While commercial concentration is not unique to quantum technologies, the exceptional potential of quantum technologies, particularly quantum computers, might lead to significant 'first mover advantages' potentially resulting in monopolies and anti-competitive practices . . . .").

consolidation of talent, patents, and hardware risks creating a landscape in which smaller companies, startups, or resource-limited nations are sidelined. From research breakthroughs to commercial applications, the few entities capable of maintaining large-scale quantum platforms would stand to reap disproportionate benefits, steering the pace and direction of innovation across critical fields such as pharmaceutical discovery, climate modeling, and financial analytics. The resulting ecosystem could embed existing technological inequalities even further, as those left without meaningful access to quantum infrastructure would struggle to compete or advance their research.

This scenario mirrors previous episodes of platform dominance,[38] yet quantum computing's disruptive reach transcends the data-centric logic of recent decades. While data capitalism hinges on controlling user data and digital networks, quantum computing is grounded in harnessing unprecedented computational capacity to tackle problems once deemed infeasible. That profound leap in problem-solving power means *quantum monopolies* can influence entire domains of technology and research far beyond data markets. In other words, even though both data control and quantum gatekeeping can create uneven power structures, the latter introduces a qualitatively different layer of strategic advantage, with the potential to redefine how innovation and value are generated across multiple sectors.

Overall, each of these governance challenges underscore that quantum computing's tensions go beyond the usual legal-ethical frameworks, touching on the physical, organizational, and societal foundations that guide the technology's path. Encryption weaknesses stem not only from quantum's computational strength, but also from the networks and standards that transfer and protect information. IP disputes involve more than intangible legal protections, as they also hinge on the materials, supply chains, and global partnerships enabling quantum R&D. Similarly, the risk of quantum monopolies resides in restricted expertise, costly hardware, and facility ownership, all of which shape who can access and exploit quantum technology. Consequently, strategies to govern quantum computing must address these infrastructural dimensions from the outset. Unless policy efforts go beyond generic regulations or ethical principles, the transformative promise of quantum computing could devolve into a new era of monopolies and inequalities.

[38] *See, e.g.,* Sara Myers West, *Data Capitalism: Redefining the Logics of Surveillance and Privacy*, 58 BUS. & SOC'Y 20, 20–21 (2019) (highlighting how the "commoditization of our data enables an asymmetric redistribution of power" to the hands of actors who can access and make sense of digital information in our current data capitalism).

IV. GLOBAL QUANTUM LAW

Quantum innovation is unfolding within a distinctly global architecture and supply chain, marked by high levels of cross-border collaboration and interdependence that build upon—and in some cases amplify—earlier technological revolutions.[39] This dynamic has given rise to a nascent transnational legal regime comprising both formal legal instruments and technical governance strategies—what this commentary refers to as *global quantum law*. Unlike some previous governance approaches to technological shifts, such as digital platforms or artificial intelligence (AI), which largely emphasized ethical principles in their formative stages, global quantum law is taking shape through early decisions about system design and deployment. Although this legal landscape remains entangled with broader normative frameworks aimed at guiding quantum technologies,[40] this commentary contends that it is these deployment-oriented governance mechanisms that are actively defining a new transnational sphere of authority over quantum infrastructures. The following section offers a concise overview of how this dynamic is materializing through several emerging global initiatives.

First, international SDOs have begun creating frameworks to guide the technical evolution of quantum technology. This trend is exemplified by several distinct albeit compounding efforts. In 2023, the ISO and IEC jointly formed a *Quantum Technologies Committee* to develop standards

[39] Researchers and companies working on quantum algorithms, error-correction techniques, or qubit designs span multiple jurisdictions and form cross-border consortia, while building and operating quantum devices often requires specialized components—such as superconducting materials, cryogenic systems, or precision lasers—sourced from different countries. The high costs and risks of quantum development also encourage multinational funding arrangements, including government grants, venture capital, and consortium-based initiatives, and the implications of quantum technologies, particularly in secure communications and advanced computing, create strong incentives for global collaboration and deployment. *See Quantum Technologies Flagship,* EUROPEAN COMMISSION, https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship (last visited Apr. 27, 2025) (describing Europe's coordinated efforts to develop and standardize quantum infrastructure, and highlighting the global interconnectedness of quantum research, hardware production, and supply chains); Antonio Acín et al., *The Quantum Technologies Roadmap: A European Community View*, 20 NEW J. PHYSICS 1, 3 (2018), https://doi.org/10.1088/1367-2630/aad1ea (highlighting that one "[s]uccess factor for the rapid advancement of QT is a well-aligned global research community with a common understanding of the challenges and goals.").

[40] *See generally* Kop, *supra* note 8 (providing a list of ten legal-ethical principles for the development of quantum technology).

on quantum computing, communications, metrology, and more.[41] Their goal is to establish a shared technical language and reference architectures that foster interoperability and safety, while also defining both feasible and desirable targets for quantum infrastructures. In a similar move—spurred by mounting cryptographic threats—the International Telecommunications Union (ITU) published its Y.3800-series recommendations, already addressing security standards and key distribution networks to integrate quantum protocols into existing telecom infrastructure.[42] National organizations like NIST in the United States and the European Telecommunications Standards Institute (ETSI) in the EU have likewise taken on significant roles in formulating quantum security strategies. Notably, NIST leads a global initiative to standardize post-quantum cryptography (PQC) algorithms for encryption and digital signatures,[43] while ETSI's Industry Specification Group on Quantum Key Distribution (ISG-QKD) has issued guidelines and certifications aimed at fortifying quantum communication networks.[44]

Yet it is important to keep in mind that such standard-setting processes do not unfold in neutral or purely technical spaces. In theory, technical standards are developed through iterative, consensus-driven processes within international and national SDOs (e.g., ISO, IEC, NIST), where working groups composed of industry representatives, researchers, and regulators propose technical specifications, revise drafts in response to stakeholder feedback, and eventually formalize them through structured voting procedures. In practice, however, standard-setting often involves a constellation of actors that do not necessarily act in coordination, including self-regulatory organizations (SROs), government procurement entities, sector-specific regulators (e.g., in finance, telecom, health), and consultants who mediate between technical committees and industry needs. Similarly, private certification bodies and training organizations help translate standards into practice, often through pay-to-play models that reproduce access disparities under the rhetoric of technical competency. These actors collectively shape how standards are drafted, interpreted, and operationalized,

[41] IEC & ISO, *IEC and ISO Launch New Joint Technical Committee on Quantum Technologies*, ISO (Jan. 11, 2024), https://www.iso.org/news/new-joint-committee-quantum-technologies.

[42] *Standards Bodies to Coordinate Contributions to Quantum Information Technology*, ITU (Mar. 17, 2021), https://www.itu.int/hub/2021/03/standards-bodies-to-coordinate-contributions-to-quantum-information-technology/.

[43] *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*, NIST (July 5, 2022), https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

[44] *Quantum Key Distribution (QKD)*, ETSI, https://www.etsi.org/technologies/quantum-key-distribution (last visited Apr. 27, 2025).

effectively creating a governance system that steers technological development in favor of better-positioned members.[45]

Second, new bilateral and multilateral agreements are increasingly coordinating international efforts in quantum infrastructure, a reflection of the inherently cross-border nature of large-scale quantum initiatives. The United States for example, has established bilateral agreements with Japan, the U.K., Australia, Finland, Sweden, France, and others, promoting shared principles for quantum research, knowledge exchange, and security protocols.[46] Significantly, these accords also set the stage for future frameworks governing cross-border quantum communication networks and data flows. Meanwhile, the EU's EuroQCI (European Quantum Communication Infrastructure) project aims to build a secure quantum communication network

[45] For example, procurement standards for quantum hardware, particularly in sensitive sectors like defense and healthcare, can embed implicit preferences for domestic vendors or create compliance thresholds that exclude smaller foreign firms from participating in supply chains. Notably, government-imposed export controls in the United States, frequently oriented toward countering Chinese technological advancement, have constrained international collaboration and complicated cross-border partnerships that smaller quantum firms depend on to scale. While framed as national security measures, such restrictions can also serve industrial protectionist aims, reinforcing the advantages of incumbent actors with the legal, logistical, and financial capacity to navigate complex regulatory environments; thereby limiting competition and innovation at the margins of the sector. Jess Weatherbed, *U.S. Expands Export Blacklist to Keep Computing Tech Out Of China,* THE VERGE (Mar. 26, 2025), https://www.theverge.com/news/636277/us-chinese-export-restrictions-blacklist-80-companies; Sam Howell, *To Restrict or Not to Restrict, That Is the Quantum Question*, LAWFARE (Sept. 11, 2024), https://www.lawfaremedia.org/article/to-restrict-or-not-to-restrict-that-is-the-quantum-question.

[46] U.S. Department of State, *Tokyo Statement on Quantum Cooperation*, (Dec. 19, 2019), https://2021-2025.state.gov/tokyo-statement-on-quantum-cooperation/; Australian Government, Department of Industry, Science, and Resources, *Joint Statement of the United States of America and Australia on Cooperation in Quantum Science and Technology*, (Nov. 19, 2021), https://www.industry.gov.au/publications/joint-statement-united-states-america-and-australia-cooperation-quantum-science-and-technology; Department for Business, Energy & Industrial Strategy & George Freeman MP, *New Joint Statement Between UK and US to Strengthen Quantum Collaboration*, GOV.UK (Nov. 4, 2021), https://www.gov.uk/government/news/new-joint-statement-between-uk-and-us-to-strengthen-quantum-collaboration; *The United States and Finland Move to Strengthen Cooperation in Quantum*, NATIONAL QUANTUM INITIATIVE (Apr. 6, 2022), https://www.quantum.gov/the-united-states-and-finland-move-to-strengthen-cooperation-in-quantum/; U.S. Department of State, *Joint Statement of the United States of America and Sweden on Cooperation in Quantum Information Science and Technology*, (Apr. 12, 2022), https://2021-2025.state.gov/joint-statement-of-the-united-states-of-america-and-sweden-on-cooperation-in-quantum-information-science-and-technology/; U.S. Department of State, *Joint Statement of the United States of America and France on Cooperation in Quantum Information Science and Technology*, (Mar. 17, 2023), https://2021-2025.state.gov/joint-statement-of-the-united-states-of-america-and-france-on-cooperation-in-quantum-information-science-and-technology/.

among member states, effectively standardizing access and security requirements at the regional level.[47] This coordination extends to the EuroQCI Space Segment—an international consortium under the European Space Agency designed to distribute encryption keys globally, thereby embedding governance into the very architecture of emerging quantum infrastructures.[48]

Public-private consortia and collaborative industry initiatives further reinforce these standards and international agreements by developing shared guidelines, reference designs, and best practices that governments increasingly adopt. For instance, entities such as the Quantum Economic Development Consortium (QED-C) in the U.S. and the European Quantum Industry Consortium (QuIC) serve as platforms where industry stakeholders, researchers, and policymakers align on technical roadmaps, define sector-specific benchmarks, and jointly address questions of interoperability.[49] As before, these efforts concentrate on the foundational infrastructure enabling quantum computing's effective cross-border integration, rather than on the underlying ethical principles it may embody.

Finally, international security alliances and global institutions are broadening their focus on quantum's strategic and infrastructural dimensions, moving beyond conventional policy statements to address the social, organizational, and technical layers essential for sustaining this technology. For example, in its 2023 quantum technology strategy, NATO emphasized quantum-resistant communications and proactive measures to mitigate hostile applications—recognizing that large-scale quantum deployment demands not only sophisticated engineering but also cross-border security

[47] *The European Quantum Communication Infrastructure (EuroQCI) Initiative*, EUROPEAN COMMISSION, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (last visited Apr. 27, 2025).

[48] *ESA and European Commission to Build Quantum-Secure Space Communications Network*, EUROPEAN SPACE AGENCY, (Jan. 30, 2025), https://www.esa.int/Applications/Connectivity_and_Secure_Communications/ESA_and_European_Commission_to_build_quantum-secure_space_communications_network.

[49] Quantum Economic Development Consortium (QED-C), *About QED-C*, QED-C, https://quantumconsortium.org (last visited Apr. 27, 2025); European Quantum Industry Consortium (QuIC), *Introduction to the Quantum Flagship*, QED-C, https://qt.eu/about-quantum-flagship/ (last visited Apr. 27, 2025); Quantum Economic Development Consortium (QED-C), *Quantum Consortia QIC, QED-C, Q-STAR and QuIC Form International Council to Enable and Grow the Global Quantum Industry*, QED-C (Jan. 31, 2023), https://quantumconsortium.org/quantum-consortia-qic-qed-c-q-star-and-quic-form-international-council-to-enable-and-grow-the-global-quantum-industry/; Abhishek Purohit et al., *Building a Quantum-Ready Ecosystem*, 5 IET QUANTUM COMMC'N, 1, 10–13 (2023).

frameworks.[50] Likewise, the UN Secretary-General's recent warnings about the disruptive potential of powerful quantum machines point to broader governance concerns, where equitable access to secure quantum infrastructure could become vital for international stability.[51] These intertwined initiatives reflect a growing consensus that quantum computing must be treated as a holistic infrastructure project—one that unites technical, organizational, societal, and legal dimensions of technological governance.

Collectively, these intertwined efforts reflect a proactive approach that addresses critical security concerns and sets technical priorities at a relatively early stage in quantum's development, even before many core components have fully matured or become widely adopted. Indeed, rather than allowing *de facto* standards to emerge organically through market forces alone, international actors and bodies are already deliberately shaping design and deployment choices. In doing so, they are trying to define the fundamental parameters within which quantum infrastructure will evolve. While market forces will still play a role as the technology rolls out, standard-setting is explicitly aiming to ensure that interoperability, safety, and cryptographic resilience remain central to its trajectory. Yet this, too, reflects a particular vision of the future, one advanced through institutions that often reproduce existing asymmetries of influence.

V. BALANCING QUANTUM PROMISE AND POWER

The initiatives described above reflect a growing recognition of quantum computing's global and infrastructural character. However, ensuring safety and interoperability alone will not be sufficient to address the deeper power asymmetries that have historically accompanied technological shifts.[52] Without more inclusive and redistributive governance approaches, current efforts risk reinforcing existing hierarchies through new technical architectures that concentrate power in the hands of a few. As this commentary has outlined, quantum computing's disruptive potential spans multiple sectors and stands to become a foundational technology, reorganizing

[50] *NATO Releases First Ever Quantum Strategy*, NATO (Jan. 17, 2024), https://www.nato.int/cps/en/natohq/news_221601.htm.

[51] Vibhu Mishra, *Humanity's Fate Can't Be Left to Algorithms, UN Chief Tells Security Council*, UN NEWS (Dec. 19, 2024), https://news.un.org/en/story/2024/12/1158376.

[52] For discussions of power imbalances in recent digital transformations, *see generally* Cohen, *supra* note 10 (discussing digital inequalities under informational capitalism); Myers West, *supra* note 40 (discussing the political economy of data capitalism); and OECD, *supra* note 30 (discussing first-mover advantages in emerging technologies, particularly in the context of quantum computing).

the relationship between societies and both physical and digital systems. Yet this promise is emerging within a global political economy marked by sharp inequalities in technological capacity, investment, and influence. Quantum computing, with its capital-intensive demands and high barriers to entry, is unlikely to be an exception. As a result, access to the benefits of quantum computing continues to be—and is likely to stay—concentrated among a small group of well-resourced states and corporations.

This raises a hard question: is there truly a window for meaningful intervention? Unlike previous waves of digital transformation, where governance often lagged far behind technical deployment, quantum infrastructure is still under construction. Standards, architectures, and regulatory frameworks are being drafted in parallel with hardware development. In principle, this synchronicity could offer an opportunity to shape quantum's future through more equitable and inclusive designs. Yet so far, most of these decisions have reinforced the advantages of already-dominant actors. International agreements, despite their cooperative framing, tend to involve a narrow set of wealthy and geopolitical partners. Global standard-setting initiatives emphasize interoperability but often fail to address the underlying inequalities that limit meaningful participation from under-resourced countries and institutions. Even industry-led consortia that aim to broaden access often operate within ecosystems where capital, expertise, and proprietary control remain highly concentrated. These developments mirror recent cases, such as AI governance, where early regulatory efforts have failed to counteract the gravitational pull of dominant actors and entrenched inequities.[53]

If we are to build a different future, meeting these challenges will require strategies that move beyond market coordination and abstract ethical statements. In fact, a more direct engagement with the political economy of quantum development is necessary. There are many possible paths in that direction. International institutions and national governments could support open licensing frameworks for foundational quantum technologies, expand public investment in quantum infrastructure accessible across borders, and create targeted funding streams for researchers in underrepresented regions. Structured technology transfer programs—drawing on experiences from global health and climate sectors—could also help reduce disparities in equipment, knowledge, and manpower. Legal frameworks that incentivize collaborative innovation and prevent excessive concentration of IP would further help resist monopolistic outcomes. While such approaches must undoubtedly account for national security risks, those concerns should not

[53] Kevin Wei et al., *How Do AI Companies "Fine-Tune" Policy? Examining Regulatory Capture in AI Governance* (Sept. 20, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4931927 (presented at the 2024 AAAI/ACM Conference on AI, Ethics, and Society).

serve as a shield for the consolidation of quantum capabilities within a narrow geopolitical or corporate elite. On the contrary, equitable governance is essential to global security and long-term stability. Yet if recent history is any guide, existing power structures will likely adapt these tools to preserve their advantage rather than dismantle it. Without sustained and intended pressure, redistribution will remain a rhetorical gesture, not a structural commitment. The window for shaping quantum governance may be open, but the mechanisms capable of prying it wide are still missing—or already being quietly closed.

The early decisions being made today regarding inclusion, access, and benefit-sharing will shape the quantum future for decades to come. Whether this future deepens inequality or expands opportunity will depend on whether global governance frameworks are equipped to treat quantum computing not only as a technical advance, but also as a transformative economic and political development.

VI. CONCLUSION

This commentary has argued that quantum computing's most urgent regulatory needs lie not in abstract ethical guidance alone, but in its infrastructural dimensions. By emphasizing design and deployment choices, from cryptographic standards to manufacturing pipelines, stakeholders might address the physical, organizational, and societal complexities that define quantum's potential. Crucially, this approach is already taking hold: international bodies, bilateral agreements, industry consortia, and security alliances are embedding technical oversight into quantum development from the outset. As a result, a transnational field of *global quantum law* is emerging—one that aligns engineering architectures with shared governance goals across jurisdictions.

Yet it remains too early to tell whether these frameworks will prevent power imbalances or mitigate unforeseen risks as the technology evolves. The sheer complexity of quantum systems, compounded by competing national and corporate interests as well as its high development and deployment costs, will challenge regulators and innovators alike. The choices we make today regarding investment, standardization, and inclusion will resonate for decades, shaping how quantum computing is produced and who benefits from it. In this light, the infrastructural lens offers not just a blueprint for technical regulation, but a space to reflect on whether quantum's unprecedented promise can be harnessed to expand societal benefit rather than deepen existing divides. Ultimately, the most pressing question for the next phase of quantum computing is how to ensure that it does not replicate the exclusions of the past.