FORD SCHOOL
SCIENCE, TECHNOLOGY,
AND PUBLIC POLICY
UNIVERSITY OF MICHIGAN

March 2026

Understanding Quantum Computing and Its Policy Implications

Saima Rashid, MPP, MS Environment & Sustainability '27

INTRODUCTION

Quantum computing (QC), once considered simply a part of theoretical physics, has advanced rapidly in the last few decades. The QC industry has entered the "utility era," where quantum systems are beginning to demonstrate practical advantages for specific real-world applications.[1] This horizon scanning memo attempts to explain the QC landscape, including significant players; applications for different industries; and the challenges QC presents to our existing technological, regulatory, and social frameworks. As we witness companies like IBM charting ambitious roadmaps toward fault-tolerant quantum systems by 2029, it is crucial to address fundamental questions about harnessing this technology's potential while mitigating its risks.[2]

What is Quantum Computing?

While traditional or "classical" computers process information in definitive bits of 0s and 1s, quantum computers use quantum mechanics principles—superposition, entanglement, and interference—to process information in quantum bits, or "qubits," which can exist in multiple states simultaneously. This is a transition from the binary world of classical computers to more complex systems with orders of magnitude more computational power.[3] The difference can be explained by the following analogy—classical computing is like navigating a maze by trying every path sequentially until finding the exit. QC, by contrast, can be imagined as exploring all the possible paths simultaneously to find the optimal exit path. This ability to estimate all possibilities at once enables quantum computers to tackle problems exponentially faster than their classical counterparts.

KEY FINDINGS

- Quantum computing (QC) operates very differently from classical computing and offers practical uses spanning from healthcare and drug development to digital security applications.
- Theoretically, hybrid AI-Quantum algorithms promise bidirectional benefits through which AI would enhance the consistency and reliability of quantum systems, while quantum computers amplify the processing power of AI to analyze vast amounts of data.
- QC will likely exacerbate existing harms associated with AI, such as algorithmic bias, misinformation, and threats to democratic institutions, by enabling AI systems to operate faster, on a larger scale, and in real-time.
- Recent advances in quantum computers pose significant cybersecurity threats, including to individual data privacy, as they can potentially break current encryption methods.
- Quantum computers require extreme conditions to function and will have a large environmental footprint as they scale up.

Furthermore, QC is not simply "faster computing." It is a paradigm shift in how computers process information. With this new way of processing information, QC can solve complex optimization problems, simulate molecular interactions, and process vast datasets more efficiently than classical systems. However, they require extreme operating conditions to function—typically temperatures near absolute zero (-273°C)—and sophisticated error-correction systems to protect the qubits' extraordinarily fragile integrity.[4]

What Does a Quantum Computer Look Like?

A modern quantum computer bears little resemblance to an everyday computer or laptop. It looks more like a science fiction physics experiment, with its maze of metal tubes, wires, and shiny components, all housed within a protective glass case to shield these components from dust and environmental disturbances. The computer itself, the quantum processor, houses all the qubits, and everything else is dedicated to cooling it down.

The most advanced quantum computers today, like IBM's quantum processors, operate at temperatures colder than outer deep space, near absolute zero at approximately 15 millikelvin. These systems require massive specialized refrigerators that run on helium, often standing taller than a person, surrounded by layers of shielding to protect the delicate quantum states from the slightest environmental interference.[5]

What Is a Quantum Computer Made Of?

Companies use different materials and design approaches depending on their distinct business models, market opportunities, and resources. For instance, IBM and Google use minerals, like aluminum, and superconducting gate-based approaches to leverage their existing semiconductor manufacturing capabilities. IonQ and Quantinuum have developed trapped-ion systems which require sophisticated optical and electromagnetic control systems, positioning these companies as providers for applications requiring maximum accuracy.[6] D-Wave uses quantum annealing, a special method to optimize large-scale problems. Lastly, PsiQuantum and Xanadu are exploring photonic approaches because of their potential to operate at room temperature, hoping to eliminate expensive cooling infrastructure that limits quantum computer accessibility.[7]

Major Players in the Field

As of mid-2025 major players such as IBM, Google, Microsoft, Amazon, D-Wave, IonQ, and Quantinuum are making rapid progress toward commercial and research-ready quantum platforms, both in the US, and globally. This marks a significant shift from purely experimental prototypes to systems capable of solving meaningful problems (as discussed in some of the applications above).

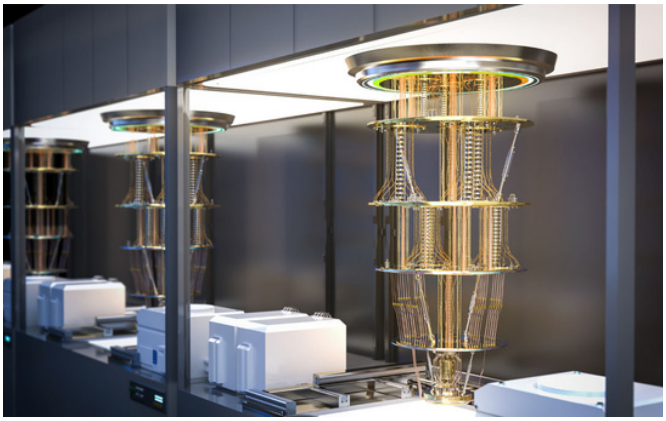

Photo credit: Phonlamaiphoto - stock.adobe.com

IBM, as a pioneer in the technology, has 15+ utility scale quantum systems established worldwide, and the company demonstrated a complete execution of a quantum circuit in 2024.[8] Google, another major player, has made significant progress in quantum error correction through Willow Chip, which was announced in 2024.[9] This expedited the quantum race, with the other two major players—Microsoft and Amazon—launching their quantum chips shortly after. In addition to the big industry giants, there is also a boom of smaller enterprises in the US, such as IonQ, Rigetti, PsiQuantum, and Xanadu, each building its own specialization in the field.

Consumer Access and Cloud Deployment

Quantum systems remain largely inaccessible to the general public due to their complexity and cost. Cloud deployment, where organisations can pay to use centrally managed quantum computing resources rather than having to own and operate expensive hardware, allows for some democratization of access. IBM is experimenting with cloud-based access through its Quantum Platform; this provides access to quantum computers, documentation, and learning resources, allowing researchers, students, and curious individuals to experiment with quantum algorithms without owning quantum hardware.[10]
Amazon and Google have their own versions of providing public access. Amazon Braket is experimenting with commercial QC services across multiple hardware providers, allowing businesses to test quantum solutions without committing to specific platforms.[11] Google Quantum AI is supporting research collaboration through development tools and educational resources.[12]

PRACTICAL USE CASES OF A QUANTUM COMPUTER

The applications of quantum computing go beyond theoretical curiosity in academics and have a significant ability to alter aspects of human life.

Use Case 1 - Medical and Pharmaceutical Applications

Recent researchers have successfully applied quantum algorithms to real-world drug discovery challenges. Scientists at St. Jude Children's Research Hospital found potential molecules for a currently untreatable type of cancer (KRAS mutation) through quantum-enhanced molecular screening. This was the first practical application of quantum computing to identify drug candidates for previously "undruggable" targets.[13] Quantum systems also have applications in personalized medicine, where they can model complex biological processes, such as protein folding, and analyze genetic data and tailor specialized treatments for individual patients.[14]

Use Case 2 - Financial Services Applications

Even though there is skepticism about its broader commercial applications, banking industry experts expect quantum computing to offer services ranging from targeted product recommendations for consumers to faster and more precise risk scenario simulations over the next 3 to 5 years.[15] The broader financial impact of QC encompasses improvements in larger systemic risk management frameworks. Financial institutions, such as JPMorgan Chase, have started using quantum computing to optimize risk analysis for investment portfolio management. Algorithms like the Quantum Approximate Optimization Algorithm (QAOA) can analyze vast numbers of investment scenarios simultaneously, enabling more sophisticated risk-return optimization than classical computing approaches.[16]

Photo credit: Phonlamaiphoto - stock.adobe.com

Use Case 3 - Cybersecurity Applications

QC introduces both challenges and opportunities in the field of cybersecurity. It poses a serious threat to current encryption models built on RSA (Rivest-Shamir-Adleman Algorithm), which is the oldest public-key cryptography algorithm used for secure data transmission, and elliptic curve cryptography, which secures everything from digital communications to financial transactions. The timeline of this vulnerability remains uncertain. According to the National Institute of Standards and Technology (NIST), these breaches might occur as soon as 2030.[17] In contrast, QC is also the antidote to the security breaches. It is expected to be able to create communication channels that cannot be broken into if they detect even the slightest attempt of eavesdropping. It will also likely enhance the authentication protocols to increase security guarantees that are not possible at the moment, such as the Quantum Good Authentication Protocol (QGP) which theoretically ensures a quantum-resistant system that enhances privacy and security.[18]

Use Case 4 - Artificial Intelligence Integration Applications

AI and QC are individually powerful, and the convergence of both offers possibilities that were beyond comprehension a few years ago. Theoretically, the integration of QC and AI creates a mutually strengthening relationship. In some cases, AI has been shown to enhance the performance and reliability of quantum systems, while quantum computing may eventually build the capabilities of AI beyond classical limits. Initial

experimentation with the hybrid models has shown promise, as they are outpacing classical supercomputers in specific complex machine learning tasks.[19] For example, a team from the Max Planck Institute and Friedrich Alexander University in Germany leveraged reinforcement learning to discover new quantum error correction codes and their respective encoders, showing that AI-driven quantum error mitigation methods can significantly improve the stability and scalability of quantum processes in real time.[20] Google's TensorFlow Quantum project is another example of a hybrid quantum-AI system, enabling researchers to develop models that integrate classical neural networks with quantum circuits, demonstrating how each technology can benefit from the other's strengths.[21]

In addition, a major part of the conversation around the unification of AI and QC revolves around creating energy-efficient infrastructure. There is evidence that hybrid quantum-AI systems can optimize energy systems and simulate complex processes more efficiently than classical methods.[22] While the theoretical potential is extensive, the reality is that for AI and QC to reach that phase of application and scale, the amount of critical minerals and resources, like helium, required would be substantial, with a significant environmental footprint.

GLOBAL QUANTUM STRATEGIES AND GEOPOLITICAL ORDER

QC is emerging as a new "space race," with several nations sprinting to secure leadership and build strategic assets in the domain because they see it as essential for future economic power, military strength, and technological sovereignty.

The United States

The US approach centers on ensuring government oversight while leveraging the private sector. Signed in 2018, The National Quantum Initiative Act outlined a 10-year plan for the advancement of quantum information science, focusing on public-private partnerships and workforce skills while considering the ethical, legal, and societal implications of quantum technologies. The Act also created the National Quantum Coordination Office (NQCO) to oversee federal investments and to coordinate strategy across government agencies.[23]

While this public-private partnership model has accelerated development, it has also concentrated power and quantum computing resources in the same major technology companies that possess the infrastructure and capital for large-scale quantum research, raising concerns about market concentration.

Beyond promoting innovation, the US regulatory strategy emphasizes security through targeted interventions. NIST has developed new standards for three post-quantum cryptographic algorithms: CRYSTALS-Dilithium, CRYSTALS-KYBER, and SPHINCS+, providing the foundation for transitioning critical infrastructure to quantum-safe encryption before large-scale quantum computers emerge.[24] Anticipating a strategy of "collect data now, decrypt later,"agencies like the Department of Homeland Security are already transitioning to these new standards as a proactive step to mitigate harms of a quantum future. On the international front, the US has implemented aggressive export controls on quantum technologies with potential military applications to competitors, adding Chinese quantum companies and research labs to trade blacklists.[25]

A key parallel between the US and Chinese governance models is that in both nations, access to quantum technology is concentrated in a few elite, powerful hands.

China

China has committed over $15 billion in public funding to quantum research, almost quadrupling the US investment, reflecting Beijing's strategic view of quantum technologies as a cornerstone of future military and economic power.[26] Unlike the US, China's quantum development is state-directed, with government research universities and elite public labs leading fundamental research. Private companies play a limited role, often acting as intermediaries between government-funded research and state-owned end users. Prominent scientists like Pan Jianwei have played a key role in aligning research with state priorities, achieving breakthroughs in satellite-based quantum

communication networks and photon-based quantum computing, reinforcing the strategic importance of quantum technologies in China's national agenda.[27] A key parallel between the US and Chinese governance models is that in both nations, access to quantum technology is concentrated in a few elite, powerful hands.

In response to the US export restrictions, China expanded its own controls by adding quantum encryption technology to its restricted export list and requiring government approval for any international transfer. It also restricted the export of ultra-low temperature technology essential for superconducting quantum computers, demonstrating China's recognition of quantum's strategic importance and its intent to control outbound technology flows.[28]

Europe

Europe pursues a more collaborative approach built around 5 features—research, infrastructure, ecosystem development, dual-use technologies, and skills training.[29] This integrates ethical and societal considerations into the development of emerging quantum technologies from the outset, while attempting to consolidate Europe's position as a leader in the field. The centerpiece of the EU's quantum strategy is the European Quantum Communication Infrastructure (EuroQCI), which focuses on creating a secure pan-European quantum communication network using terrestrial fiber networks and space-based systems. A quantum communication network uses quantum particles to transmit information with theoretically unbreakable security, and the EuroQCI is designed to enhance cybersecurity; support digital sovereignty; and protect strategic assets such as government institutions, hospitals, and energy grids.[30] The European Union is working closely with companies in its member states like Pasqal (France), IQM (Finland), and AQT (Austria) to develop scalable quantum technologies.[31] Rather than focusing solely on commercial competition, Europe's approach reflects its broader values of technological sovereignty, scientific excellence, and cooperative leadership.[32]

Recent advances in quantum computers pose significant threats to data privacy and security as they can potentially break the current encryption methods that protect sensitive personal information.

Other Players

In addition to these key players, there are other nations advancing distinct national strategies to build quantum capabilities aligning with their broader geopolitical goals. India adopted a National Quantum Mission in 2023; Japan launched its Vision of Quantum Future Society in 2022; and Canada is investing $360 million for research in the field.[33] The UK has adopted a regulatory sandbox model, allowing quantum technologies to be tested in controlled environments, and is working closely with its Regulatory Horizons Council to ensure that regulation supports innovation while managing emerging risks.[34]

New Technological Global Order

Given the diverse use cases of QC, from cryptography to AI, technological sovereignty is a recurring theme in quantum geopolitics as nations strive to build self-sufficiency in quantum capabilities. It has created an extremely polarized and bifurcated geopolitical order through the establishment of strategic security alliances, such as AUKUS (Australia, US, and UK) and joint China-Russia efforts; strong collaboration between these allies; and intensive rivalry with competitors. This also sets up a new stage for norms around global technological transfers.[35]

CHALLENGES, CONCERNS, AND HARMS

Technical Limitations of Quantum Computing

The biggest technical challenge that quantum computing faces is qubit decoherence, where qubits can lose stored information. Qubits are very fragile; any perturbation, such as a slight vibration or a change in temperature, referred to as quantum noise, can affect them uncontrollably. This leads to structural issues with error correction and scalability.

1. **Error Correction:** Quantum computers are highly prone to errors because qubits are extremely fragile and sensitive to quantum noise. Any slight movement or interaction with the environment can easily disrupt the system and degrade the accuracy of the computation.[36]

2. **Scalability:** Quantum systems currently operate on a small scale due to the complexity of technology, but most real-world applications would require massive scaling that existing hardware cannot yet support. Expanding quantum systems to hundreds or thousands of qubits while maintaining the coherence and low error rates necessary for reliable operation will be very difficult and resource intensive.[37]

Environmental Impact

Quantum systems have notable adverse environmental impacts.

1. **Energy demand:** Quantum computers require significant energy expenditures to maintain low-temperature and vacuum-pressure operational environments.

2. **Resource demand**: In addition to basic energy consumption, quantum computing also requires specialized materials that have consequential environmental footprints. Helium-3, critical for dilution refrigerators used in many quantum systems, is becoming increasingly scarce with growing quantum computing deployment. Similarly, rare earth metals required for superconducting components and specialized quantum sensors face severe supply constraints with serious social and environmental implications.[38]

3. **AI-QC integration costs**: To achieve scale that would actually support practical applications would also mean greater demand for data centers, leading to a larger collective environmental footprint in terms of water and energy consumption.[39]

Photo credit: Michael Evans - stock.adobe.com

Individual Privacy and Data Security Threats

Recent advances in quantum computers pose significant threats to data privacy and security as they can potentially break the current encryption methods that protect sensitive personal information.[40] A data theft strategy known as "harvest now, decrypt later" means that cybercriminals can steal encrypted data today, including individual health records, banking details, financial transactions, and private communications, and store it until quantum computers become powerful enough to decrypt it. Even multi-factor authentication protocols would be ineffective in that scenario, so there is little that individuals can do to protect themselves; it is therefore urgent that organizations follow NIST's guidance to immediately migrate to new standards.[41]

Amplifying AI Harms

QC's advanced processing capabilities will amplify existing AI harms by enabling much faster and more sophisticated data analysis.

1. **Increase in existing algorithmic biases:** QC accelerates the ability to train AI models and also aggravates the issues of biased and flawed datasets along with the challenges of misrepresentation due to data deserts, which are geographic areas characterized by a lack of high-quality, representative data. It can lead to more widespread algorithmic disparity impacting fields like healthcare and criminal justice. Even seemingly unbiased data can make incorrect correlations tied to race, gender, and socioeconomic status, perpetuating the vicious cycle of disadvantage for underrepresented groups.

2. **Rise in dissemination of false information:** The combination of both AI and QC enables the rapid generation and spread of deepfakes and misinformation at an unprecedented scale. This threatens to potentially undermine democratic processes of representation and accountability and erode public trust.

3. **Concentration of power:** With access limited to wealthy institutions and technology giants, which control both quantum and AI infrastructure, this creates a profound form of digital divide. Access to cutting-edge technology and its applications in healthcare and other sectors will be determined by wealth, privilege, and geopolitical power.[42]

4. **Increase in public surveillance:** Increased computational abilities allow the AI systems to analyze vast surveillance datasets in real time, creating sophisticated tools for profiling and monitoring individuals. This, in addition to posing civil liberties concerns, also disproportionately impacts marginalized communities, as research shows AI surveillance systems already exhibit demographic biases.[43]

QC can exacerbate harms by enabling AI systems to analyze vast surveillance datasets in real time, making privacy breaches, civil liberties violations, and discriminatory outcomes more pervasive and harder to detect.

QC amplifies existing harms associated with AI, such as algorithmic bias, misinformation, and threats to democratic institutions, while concentrating power in the hands of a few technology giants. With its advanced processing capabilities, QC can exacerbate these harms by enabling AI systems to analyze vast surveillance datasets in real time, making privacy breaches, civil liberties violations, and discriminatory outcomes more pervasive and harder to detect.

REGULATORY APPROACHES

Though it is a highly complex technology, governance challenges posed by quantum computing mirror issues in other technologies, including AI, nuclear technologies, and the internet. For ethical considerations, the European Union's AI Act can provide an initial blueprint to regulate quantum computation through safe and ethical mechanisms.[44] Nuclear technology governance provides a model for regulating a dual-use technology on an international scale. It is evident that both quantum and nuclear technologies have civilian benefits and national security applications which require governance frameworks that promote beneficial uses while preventing harm. The international atomic energy regulatory model could have some useful lessons for quantum governance, especially regarding technology transfer controls, and cooperative oversight mechanisms.

The evolution of internet governance from primarily technical coordination to encompassing privacy, security, and economic regulation can serve as an example for a holistic and comprehensive approach to regulating QC, especially the intersections of QC and AI. Further, the EU's General Data Protection Regulation (GDPR), through its principles of privacy by design and its emphasis on data security and individual rights, makes GDPR an important tool that could be used to establish global norms around responsible innovation in quantum computing.[45]

Currently, most of us do not understand or feel the presence of quantum computing in our daily lives; we are not going to have quantum laptops on our desks anytime soon. But, as with Artificial Intelligence, one can see the hype building up and rippling through domestic boundaries and international geopolitical order. At an individual level, it is vital to recognize the current pattern of delaying necessary protective measures based on anticipatory harms like data privacy, misinformation, or algorithmic bias, in the name of encouraging innovation. As evident in the case of AI or social media, regulation started when these issues were already embedded in the systems and had started affecting millions of people. In the case of quantum computing, we are still at a point where we can and should do things differently. We must enact thoughtful oversight before issues emerge, such as protections around data security, ethical use, and equitable access to quantum-safe encryption. Policymakers do not need to understand the physics; they just need to remember that guardrails should be built as a precaution, rather than a response to harm.

ENDNOTES

1. Jay Gambetta, "The hardware, and software for the era of quantum utility is here," *IBM Quantum Research Blog*, December 4, 2023, https://www.ibm.com/quantum/blog/quantum-roadmap-2033.
2. Ryan Mandelbaum et al., "How IBM will build the world's first large scale fault-tolerant quantum computer," I*BM Quantum Computing Blog*, June 10, 2025, https://www.ibm.com/quantum/blog/large-scale-ftqc.
3. Josh Schneider and Ian Smalley, "What is quantum commuting," IBM Think, https://www.ibm.com/think/topics/quantum-computing.
4. Norm Quesnel, "Cooling Quantum Computer Chips," *ATS Thermal Engineering Blog*, April 18, 2025, https://www.qats.com/cms/2025/04/18/cooling-quantum-computer-chips/.
5. Pat Gumann and Jerry Chow, "IBM scientists cool down the world's largest quantum-ready cryogenic concept system," *IBM Quantum Research Blog,* September 8, 2022, https://www.ibm.com/quantum/blog/goldeneye-cryogenic-concept-system.
6. David Cardinal, "Quantum Computing Goes Commercial with IBM's Q System One," *ExtremeTech*, January 10, 2019, https://www.extremetech.com/extreme/283427-quantum-computing-goes-commercial-with-ibms-q-system-one
7. Eric Ostby, "Networking Different Quantum Computing Platforms,"*Aliro Quantum Blog*, December 25, 2025, https://www.aliroquantum.com/blog/networking-different-quantum-computing-platforms.
8. Chris Nay, "IBM Expands Quantum Data Center in Poughkeepsie, New York to Advance Algorithm Discovery Globally," IBM Newsroom, September 26, 2024, https://newsroom.ibm.com/2024-09-26-ibm-expands-quantum-data-center-in-poughkeepsie,-new-york-to-advance-algorithm-discovery-globally.
9. Arjun Kharpal, "Google Claims Quantum Computing Milestone– but the Tech Can't Solve Real-World Problems Yet," CNBC, December 10, 2024, https://www.cnbc.com/2024/12/10/google-claims-quantum-milestone-but-cant-solve-real-world-problems-.html.
10. "Pricing," Explore products & Services, IBM Quantum, accessed January 26, 2025 , https://www.ibm.com/quantum/pricing; Josh Schneider, and Ian Smalley, "What Is Quantum Computing?," IBM Think, https://www.ibm.com/think/topics/quantum-computing.
11. "Amazon Braket," *Amazon Web Services*, accessed January 21, 2026, https://aws.amazon.com/braket/.
12. "Educational Resources," Google Quantum AI, accessed February 7, 2026, https://quantumai.google/resources.
13. Alex Generous, "Quantum Computing Makes Waves in Drug Discovery," St. Jude Children's Research Hospital, April 3, 2025, https://www.stjude.org/research/progress/2025/quantum-computing-makes-waves-in-drug-discovery.html.
14. Naveen Jeyaraman et al., "Revolutionizing Healthcare: The Emerging Role of Quantum Computing in Enhancing Medical Technology and Treatment," *Cureus* 16, no. 8 (2024), https://www.cureus.com/articles/278342-revolutionizing-healthcare-the-emerging-role-of-quantum-computing-in-enhancing-medical-technology-and-treatment#!/.
15. Elena Yndurain, Stefan Woerner, and Daniel J. Egger, "Exploring Quantum Computing Use Cases for Financial Services," IBM Institute for Business Value, September 2019, https://www.ibm.com/downloads/documents/us-en/10c31775c754010a.
16. Global Technology Applied Research, "Accelerating quantum optimization research by algorithm-specific scalable GPU simulation," *JP MorganChase Blog*, December 22, 2023, https://www.jpmorganchase.com/about/technology/blog/quantum-optimization-research.
17. Dustin Moody, Ray Perlner, Andrew Regenscheid, Angela Robinson, and David Cooper, "Transition to Post-Quantum Cryptography Standards: NIST Internal Report 8547 (Initial Public Draft)," *National Institute of Standards and Technology*, November 2024, https://doi.org/10.6028/NIST.IR.8547.ipd.
18. Paul Wang, "A Quantum Good Authentication Protocol," CSIAC, February 18, 2025, https://csiac.dtic.mil/articles/a-quantum-good-authentication-protocol/.
19. "Quantum Artificial Intelligence: Exploring the Relationship Between AI and Quantum Computing," *Cloud Security Alliance* (blog), January 20, 2025. https://cloudsecurityalliance.org/blog/2025/01/20/quantum-artificial-intelligence-exploring-the-relationship-between-ai-and-quantum-computing.
20. Jan Olle, Remmy Zen, Matteo Puviani, and Florian Marquardt, "Simultaneous Discovery of Quantum Error Correction Codes and Encoders with a Noise-Aware Reinforcement Learning Agent," *npj Quantum Information* 10, no. 126 (2024), https://doi.org/10.1038/s41534-024-00920-y.
21. Michael Broughton et al., "TensorFlow Quantum: A Software Framework for Quantum Machine Learning," Google Research, revised August 26, 2021, https://research.google/pubs/tensorflow-quantum-a-software-framework-for-quantum-machine-learning/.

ENDNOTES

22. Manal Jammal, Laura Sanz-Martín, and Javier Parra-Domínguez, "Quantum Innovations: Driving Sustainability Through AI and Quantum Technologies," in *Ambient Intelligence – Software and Applications – 15th International Symposium on Ambient Intelligence*, ed. Paulo Novais et al. (Springer, 2025), 351–59, https://link.springer.com/chapter/10.1007/978-3-031-83117-1_33.
23. National Quantum Initiative Act, H.R. 6227, 115th Cong. (2018), Public Law 115-368, https://www.congress.gov/bill/115th-congress/house-bill/6227.
24. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," National Institute of Standards and Technology, August 13, 2024, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.
25. Dylan Butts, "U.S. Rolls Out New Chip-Related Export Controls as China Makes Industry Advances," CNBC, September 6, 2024, https://www.cnbc.com/2024/09/06/us-china-quantum-chip-related-export-controls.html.
26. David Lague, "U.S. and China Race to Shield Secrets from Quantum Computers," Reuters, December 14, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-quantum/.
27. "Making Light Work of Quantum Breakthroughs," *Nature*, accessed August 14, 2025, https://www.nature.com/articles/d42473-021-00423-w.
28. Butts, "U.S. Rolls Out New Chip-Related Export Controls as China Makes Industry Advances.," CNBC, updated September 6, 2024, https://www.cnbc.com/2024/09/06/us-china-quantum-chip-related-export-controls.html.
29. "Quantum Europe Strategy," European Commission, July 02, 2025, https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy.
30. "European Quantum Communication Infrastructure- EuroQCI," European Commission, accessed August 14, 2025, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.
31. "Our Quantum Computers," European High Performance Computing Joint Undertaking (EuroHPC JU), https://www.eurohpc-ju.europa.eu/eurohpc-quantum-computers/our-quantum-computers_en.
32. Galina Misheva, "Commission launches Quantum Europe Strategy to turn EU into a Quantum Powerhouse by 2030," EU Digital Skills and Jobs Platform, July 8, 2025, https://digital-skills-jobs.europa.eu/en/latest/news/commission-launches-quantum-europe-strategy-turn-eu-quantum-powerhouse-2030.
33. National Quantum Mission," Department of Science & Technology, Government of India, accessed August 14, 2025, https://dst.gov.in/national-quantum-mission-nqm; "Vision of Quantum Future Society: Future Society to be Realized through Quantum Technology and Strategies for Its Realization," Secretariat of Science, Technology and Innovation Policy, Cabinet Office, Japan, April 2022, https://www8.cao.go.jp/cstp/english//outline_vision.pdf; "Overview of Canada's National Quantum Strategy," Innovation, Science and Economic Development Canada, last revised May 15, 2025, https://ised-isde.canada.ca/site/national-quantum-strategy/en.
34. "Regulating Quantum Technology Applications: Government Response to the RHC," Department for Science, Innovation and Technology, UK, October 8, 2024, https://www.gov.uk/government/publications/regulating-quantum-technology-applications-government-response-to-recommendations-made-by-the-regulatory-horizons-council/regulating-quantum-technology-applications-government-response-to-the-rhc.
35. Lauren Kahn "AUKUS Explained: How Will the Trilateral Pact Shape Indo-Pacific Security?" Council on Foreign Relations, updated June 12, 2023, https://www.cfr.org/articles/aukus-explained-how-will-trilateral-pact-shape-indo-pacific-security.
36. Matt Swayne, "What Are The Remaining Challenges Of Quantum Computing?" The Quantum Insider, April 21, 2024. https://thequantuminsider.com/2023/03/24/quantum-computing-challenges/.
37. "Beyond the Hype: Understanding the Limitations of Quantum Tech," Quantum Zeitgeist, January 5, 2025, https://quantumzeitgeist.com/beyond-the-hype-understanding-the-limitations-of-quantum-tech/.
38. "13 Risks That Come With the Growing Power of Quantum Computing," *Forbes*, November 8, 2022, https://www.forbes.com/councils/forbestechcouncil/2022/11/08/13-risks-that-come-with-the-growing-power-of-quantum-computing/.
39. Duc Tuan "Terry" Nguyen and Ben Green, "What Happens When Data Centers Come to Town?," Science, Technology, and Public Policy program, University of Michigan, July 15, 2025, https://stpp.fordschool.umich.edu/research/policy-brief/what-happens-when-data-centers-come-town.
40. "The Impact of Quantum Computing on Data Privacy and Security," Quantum Zeitgeist, accessed August 14, 2025, https://quantumzeitgeist.com/the-impact-of-quantum-computing-on-data-privacy-and-security/.
41. "Transition to Post-Quantum Cryptography Standards," NIST Internal Report 8547 (Draft). November 12, 2024. https://doi.org/10.6028/NIST.IR.8547.ipd.

ENDNOTES

42. Alberto Boretti, "Technical, Economic, and Societal Risks in the Progress of Artificial Intelligence Driven Quantum Technologies," *Discover Artificial Intelligence*, Vol. 4, October 7, 2024, https://link.springer.com/article/10.1007/s44163-024-00171-y.
43. Adam Zewe, "Study: AI Could Lead to Inconsistent Outcomes in Home Surveillance," MIT News, September 19, 2024, https://news.mit.edu/2024/study-ai-inconsistent-outcomes-home-surveillance-0919.
44. European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L) 1689, https://artificialintelligenceact.eu/ai-act-explorer/.
45. "General Data Protection Regulation (GDPR)," European Union, May 4, 2016, https://gdpr-info.eu.