Title

The Quantum Race: U.S.-Chinese Competition for Leadership in Quantum Technologies

Author

Krause, Juljan

Publication Date

2024-02-28

UNIVERSITY OF CALIFORNIA

The Quantum Race: U.S.-Chinese Competition for Leadership in Quantum Technologies

Juljan Krause

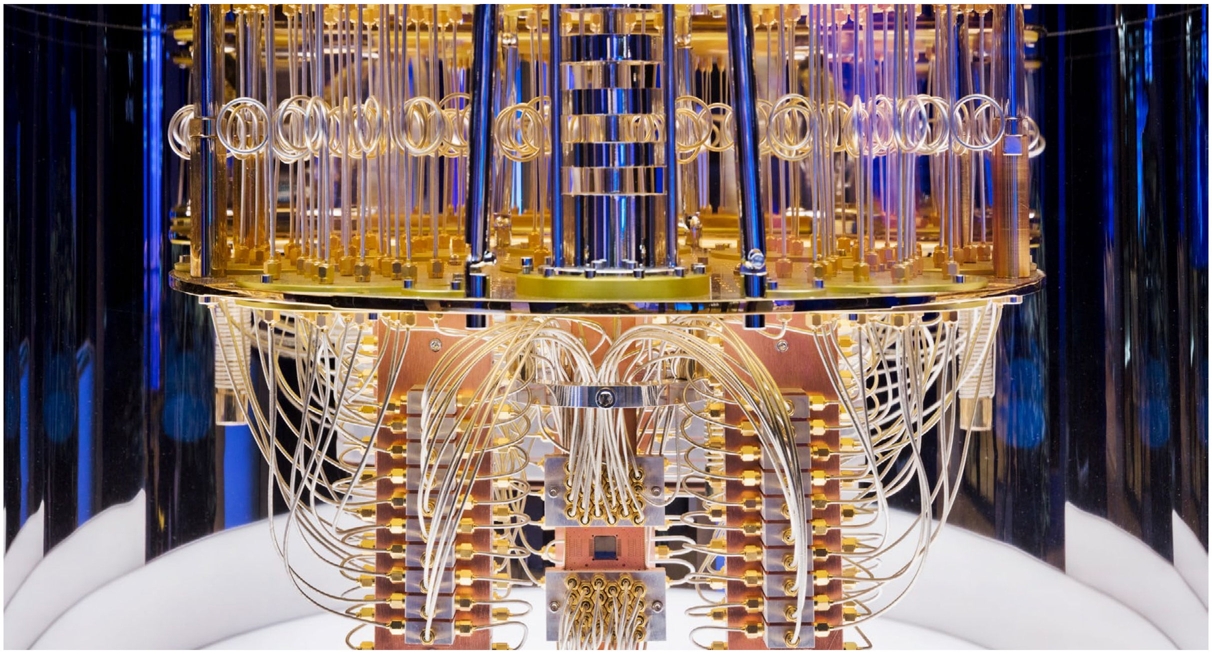
Summary

Quantum computing is poised to unleash innovation across various sectors, from materials science to pharmaceutical and medical research, finance, logistics, and even climate change management. Quantum computing has the potential to provide the backbone for future artificial intelligence (AI) and autonomous systems that cannot be realized with digital hardware alone, while quantum communication can strengthen security in cyberspace. For these reasons, quantum technologies will figure prominently in the emerging technologies race between the United States and China.

While the United States focuses on building up compute capabilities, China is advancing at pace in quantum communication. Such systems will be monumental for signaling Chinese technological leadership while protecting China's domestic communications from foreign intelligence surveillance. Chinese leadership in quantum communication will have strategic repercussions as it is likely to give China's current efforts to shape global industry standards additional momentum. Even if quantum communication has no immediate military implications, policymakers should consider how the technology could embolden China further.

IGCC

IGCC Policy Brief February 2024



Interior of an IBM quantum computing system. Photo: IBM, CC BY-ND 2.0, via Wikimedia Commons

The Promise of Quantum Computing

Global demand for computing power is growing rapidly. Increasingly sophisticated generative AI will have a significant impact across most industrial sectors, requiring an enormous volume of processing power.[1,2] The armed forces and intelligence community also require evermore complex technologies to keep pace with adversaries.[3]

Established digital computing architecture based on semiconductor technologies—which are crucial components of computers and other electronic devices that enable machines to execute commands—cannot deliver the exponential scale-up in compute capabilities that these large new systems demand.[4] The rapid growth in AI and autonomous systems will thus inevitably run into hardware limitations—since only so many transistors can be squeezed onto a chip.

Quantum systems, on the other hand, promise the ability to vastly scale up compute capability. For this reason, quantum holds a special position in the busy marketplace of emerging technologies.[5]

Given their exponential upgrade of compute power and the additional cybersecurity they provide (see Boxes 1 and 2), quantum technologies will likely provide the backbone infrastructure to accommodate future breakthroughs in AI and autonomous systems.

While quantum computers will not be better or faster across all domains, they will greatly outperform classical computing in many areas. Quantum computers will have an advantage in any field featuring large systems characterized by myriad complex interactions between variables—systems such as the economy, climate change, or astrophysics.

Quantum computers may also be able to solve problems previously considered intractable. Cryptography is an example; encryption systems that seemed unhackable may become an easy target for a quantum computer.

BOX 1.

What is Quantum Computing?

From smartphone, to laptop, to supercomputer, tiny transistors in digital machines flip back and forth between voltage levels to run apps and interpret user input. When no voltage is applied, the transistor is off; when it amplifies an electrical signal, it's on. This binary structure is represented in machine language as 0 or 1. The binary digit, known as a bit, can only ever be 0 or 1 at any one time, meaning that either a current is flowing through the transistor, or it is not. In modern computers, billions of transistors are linked together to deliver computational tasks.

Quantum computing works very differently. Here, the basic unit is called the quantum bit, or qubit. Unlike the bit, a qubit can be in two states at the same time, not just one.

The power of quantum computing becomes more obvious when several qubits interact. Two qubits can enter a peculiar kind of bond, called entanglement, to form a new, single computational unit that can hold four states simultaneously. Three qubits in entanglement can hold eight states (2^3)—the number of possible states rises exponentially with the number of qubits a quantum chip contains. As each state represents information, the number of operational tasks that a quantum computer could perform at once grows very large very fast.

There are obstacles to realizing this game-changing technology. While a classical transistor with bits is sturdy and reliable, qubits are not. Qubits are subatomic particles; as such they're very fragile and quickly disintegrate. A quantum computer requires a constant supply of replacement qubits loaded onto the chip to sustain computation. Moreover, it isn't clear which particle will make the best qubit. Some research projects aim to leverage existing silicon wafer manufacturing principles for building reliable qubits, while others use photons, trapped ions, or nitrogen vacancies in diamonds.

The physical difficulty of realizing the theoretical advantages of qubits is a fundamental challenge for quantum computing. But the potential scale-up of computing power is so large that it is worth the hassle. A quantum computer of 300 reliably performing qubits would be able to run 2^{300} computations at the same time—a figure greater than the number of particles in the entire visible universe.

China's Aim to Lead in Quantum Communication

China is outspoken about its aim to embed quantum technologies into its larger emerging technologies portfolio, which its leadership considers crucial to achieving global techno-security dominance in the 21st century.[6] President Xi Jinping is personally invested in quantum technologies, heralding the potential for China to surpass the United States in this critical area.[7]

Recent research suggests that China enjoys an edge over the United States in developing quantum communication systems, which exploit the properties of quantum objects to defend against eavesdropping (see Box 2).[8] While these early systems are clunky—and both hardware and personnel-intensive to develop, build, and service—once they mature, they will present significant challenges to Western policymakers, notably in the realm of foreign espionage.

The quality of communications intercepted by China's adversaries will diminish if the country is able to communicate internally over secure quantum channels. Chinese progress is difficult to estimate, but engineering feats such as the quantum satellite *Micius*, which enables quantum communication over vast distances and was launched in 2016, are impressive.[9] Being a satellite, *Micius* avoids some of the problems that transmitting quantum signals on the ground pose. The satellite is a signal of intent, and attests to the firm belief of senior Chinese officials that these new systems can shield internal relay against foreign espionage.

A sophisticated Chinese quantum communication system supports China's purported "Harvest Now, Decrypt Later" strategy, which siphons off large volumes of Internet traffic in the hope that it can be deciphered in the near future.[10] With other state actors assumed to be following suit, concern is growing about the fallout of an adversary being able to decode government and private sector communications.

Solar wing deployment testing for quantum satellite *Micius*.
Photo: Xinhua

One of the ways China hopes to establish global leadership is by shaping future technology standards, particularly as they relate to the Internet, computing, and network domains. To this end, Beijing has extended its influence over international standardization bodies.[11]

Chinese efforts to shape standards for quantum communication are strong signals of its ambition to dominate this emerging technology, both in terms of manufacturing and of how quantum communications will ultimately be embedded into existing systems. International standard setting has not typically been a focus of great power rivalry, but Western policymakers are waking up to an increasingly emboldened, competitive, and at times combative China in international negotiations on future technology standards.

BOX 2.

What is Quantum Communication?

Quantum computers, due to their powerful nature, reduce the difficulties and time involved in a brute-force attack, in which hackers use trial and error to break into sensitive cyber systems. Since quantum computers will run computations—and therefore attacks—very differently than traditional computers, commonly deployed encryption systems offer little protection against quantum hacking.

The best response to quantum offense is quantum defense. Researchers have developed a technology called quantum key distribution (QKD) that exploits the properties of qubits for secure communication. QKD exploits the quantum phenomena of superposition and entanglement to ensure eavesdropping is noticed by the system, thus sounding an alarm.

With QKD, the exchange of key pairs is quantum-encoded yet the message itself is exchanged through classical, non-quantum communication channels. QKD is said to be information-theoretically secure—that is, secure against hackers whose time and computing resources are unlimited. However, smart quantum hackers have already exploited weaknesses at endpoints where QKD links to legacy hardware. On top of such practical issues of implementation, the U.S. National Security Administration and Britain's GCHQ intelligence service, warn that QKD comes with its own security challenges, such as a greater risk from insider threats.

U.S. and Western interests

Given the critical role of quantum technologies for future research and development (R&D), there are vast incentives for China to be the first to offer novel quantum systems, and China has emerged as a serious contender for global technological leadership. Beijing is vocal about challenging the dominance of Western digital technologies and rewriting the standards that govern them. For Chinese policymakers, leadership in advanced technologies—especially those that are critical to national security—are instrumental to realizing what Xi Jinping calls the Chinese dream of "national rejuvenation."[12]

Due to their potential to radically upset the global computing landscape, quantum technologies enjoy a particularly important status in the accelerating innovation race between the United States and China. A competitive edge in building up quantum capabilities may translate in a first-mover advantage for Chinese corporations to build a global client base for quantum compute services. Leadership in quantum engineering may also give China a boost in international forums and organizations tasked to find standards and governance models for future quantum systems, which may force American industry to abide by Chinese rules. The United States and its allies have a significant strategic interest in containing Chinese progress in quantum technologies.

The United States has responded to Chinese quantum ambition in various ways. The National Quantum Initiative Act of 2018 formulated an initial response to the strategic challenges that quantum technologies pose.[13] Initial funding of $1.2 billion was distributed across several research centers and consortia, aiming to make the United States a world leader in quantum computing.[14]

The Biden administration has upped its efforts to communicate just how important the government considers quantum technologies to be. In the National Security Memorandum of May 2022, President Biden emphasized that it is the policy of his administration "to maintain United States leadership in quantum information science."[15]

Today, the United States is generally considered the global leader in quantum computing, due to a diverse and efficient R&D ecosystem that matches private sector ambition with highly skilled and motivated university trained talent.[16] Europe, on the other hand, has established an impressive record in other quantum technologies such as quantum sensing and metrology, with funding from the European Union's €1.6 billion Quantum Flagship initiative.[17]

The United States and the United Kingdom consider the protection of domestic intellectual property rights to be a pressing issue. Quantum technologies sit alongside other critical emerging technologies, such as AI, autonomous systems, robotics, and hypersonics, which the White House considers "of particular importance to the national security of the United States."[18]

The specter of Chinese entities siphoning off hard-earned innovation looms large. This threat motivated the directors of the foreign intelligence services of the Five Eyes intelligence-sharing alliance between the United States, United Kingdom, Canada, Australia, and New Zealand to appear together publicly in October 2023 to warn about the scale and sophistication of Chinese industrial espionage, a first for the alliance.[19]

IBM Quantum Lab. Photo: Connie Zhou for IBM, CC BY-ND 2.0, via Wikimedia Commons

Western governments believe it is urgent to make headway in post-quantum cryptography. Indeed, some of the risks to network security that quantum networks may pose are actively being tackled by the U.S. Department of Commerce's National Institute of Standards and Technology. The booming field of post-quantum cryptography has attracted a steady stream of funding and has already delivered novel encryption systems that will hold up even against powerful quantum machines.[20]

While quantum communication has been left to China, U.S. leadership in quantum computing is supported by the dominance of American tech heavyweights that enjoy incumbent leadership positions in the high-performance and cloud computing markets. Alphabet, Amazon, IBM, and Microsoft are investing heavily in quantum capabilities, hoping to offer customers future quantum resources over the cloud.

While the United States' ability to involve the private sector in developing technologies critical to national security is unrivaled, overreliance on the private sector presents its own challenges, such as new structural dependencies on a small number of powerful corporations. With new quantum capabilities added to their portfolio, U.S. Big Tech is likely to further cement its position as a strong political actor.

Policy implications

The prospect of a strategic adversary realizing substantial quantum computing breakthroughs first is alarming. Quantum technologies provide an opportunity for China to present to the world a genuinely Chinese computing technology. The ramifications of China securing a first-mover advantage are considerable. It would offer an immense reputational asset to Beijing, strengthen Chinese efforts to dominate standard-setting for critical network technologies, and provide new attack vectors for government-sponsored cyber campaigns against foreign assets.

Three major themes emerge for policymakers. Regarding government relationships with the private sector, if the same companies which already dominate the global cloud computing market are going to offer quantum compute resources over the cloud, existing structural dependencies on these companies may solidify. This would increase risk levels for the U.S. economy and the government alike. The Federal Trade Commission in the United States and the Competition and Markets Authority in the United Kingdom have begun investigating potential competition concerns in the provision of cloud computing services.[21, 22] Additional consideration of how quantum technologies may further consolidate market power in cloud computing would help future-proof current efforts.

Quantum technologies emerge at a time when AI is improving at an accelerated rate. Quantum computing systems may provide new hardware to accommodate AI while quantum machine learning may yield new types of algorithms that make AI faster still. Generative AI and autonomous systems are widely assumed to significantly impact all industrial sectors. The diffusion and ultimate success of these systems will not only depend on finding new algorithms, but also on building the backbone infrastructure that can accommodate these systems. While the former is being discussed at length, the issue of system-critical limitations of digital computing technologies has not captured the level of attention it deserves. Strategic considerations of how quantum capabilities could help address these concerns seem warranted.

With a view towards China's technological leadership ambitions, the immediate security risks of Chinese quantum communication systems are likely to prove manageable. However, Chinese progress in this domain presents wider challenges. The signaling effects of Chinese leadership in quantum communication may give momentum to Beijing's efforts to shape future telecommunications and Internet standards in international bodies, adding to Chinese soft power. Whether or not quantum communication is of immediate military use, Chinese innovation in this critical domain is likely to give its technology program significant credibility at home and abroad.

Conclusion

The emergence of quantum computing comes amid intensifying competition over emerging technologies between the United States and China. While the United States enjoys a leadership position overall, China has made remarkable progress. The United States' chief strategic rival seems particularly focused on realizing quantum communication technologies that may offer unprecedented levels of security—if it can overcome issues around integrating quantum with legacy digital infrastructure.

Chinese leadership in quantum technologies could pose a threat to Western interests, particularly with regards to intellectual property rights and standard setting for future computing technologies. The United States and its allies should continue to invest in quantum research while attending to potential regulatory and competition concerns that quantum technologies are likely to present. Long-term success in the quantum domain requires Western policymakers to confidently meet Chinese ambition while ensuring that domestically, quantum technologies can benefit the economy beyond large private-sector players.

Endnotes

1. Adam Zewe, "Explained: Generative AI," *MIT News*, November 9, 2023, https://news.mit.edu/2023/explained-generative-ai-1109.

2. *The Impact of Artificial Intelligence on the Future of Workforces in the European Union and the United States of America: An economic study prepared in response to the US-EU Trade and Technology Council Inaugural Joint Statement,* White House and European Commission issue brief, December 5, 2022, https://www.whitehouse.gov/cea/written-materials/2022/12/05/the-impact-of-artificial-intelligence/.

3. Juljan Krause, *Trusted autonomous systems in defence: A policy landscape review*, The Policy Institute at King's College London report, November 18, 2021, https://kclpure.kcl.ac.uk/portal/en/publications/trusted-autonomous-systems-in-defence-a-policy-landscape-review.

4. Andrew Zola, "DEFINITION: semiconductor," *TechTarget*, last updated November 2021, https://www.techtarget.com/whatis/definition/semiconductor.

5. "Stanford Emerging Technology Review: Reporting on Key Technology Areas and their Policy Implaications," Stanford University, accessed February 7, 2024, https://setr.stanford.edu/.

6. "China becomes 3rd country to deliver quantum computers, after Canada and US," *Global Times*, January 30, 2023, https://www.globaltimes.cn/page/202301/1284467.shtml.

7. Elsa B. Kania, "China's Quantum Future: Xi's Quest to Build a High-Tech Superpower," *Foreign Affairs*, September 26, 2018, https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future.

8. Edward Parker et al., *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*, RAND Corporation report, 2022, https://www.rand.org/pubs/research_reports/RRA869-1.html.

9. Chao-Yang Lu et al., "Micius quantum experiments in space," *Reviews of Modern Physics* 94, 035001, July-September 2022.

10. Kevin Townsend, "Solving the Quantum Decryption 'Harvest Now, Decrypt Later' Problem," *SecurityWeek*, February 16, 2022, https://www.securityweek.com/solving-quantum-decryption-harvest-now-decrypt-later-problem/

11. Bradley A. Thayer and Lianchao Han, "We cannot let China set the standards for 21st century technologies," *The Hill*, April 16, 2021, https://thehill.com/opinion/technology/548048-we-cannot-let-china-set-the-standards-for-21st-century-technologies/.

12. "Xi Focus: Xi Jinping on rejuvenation of Chinese nation," *Xinhua*, October 11, 2020, http://www.xinhuanet.com/english/2020-10/11/c_139431888.htm.

13. "H.R.6227 - National Quantum Initiative Act, 115th Congress (2017-2018)" Congress.gov, last accessed February 7, 2024, https://www.congress.gov/bill/115th-congress/house-bill/6227.

14. "National Quantum Initiative," U.S. National Quantum Coordination Office, last accessed February 7, 2024, https://www.quantum.gov/.

15. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," The White House, May 4, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

16. Edward Parker et al., An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology, RAND Corporation report, 2022, https://www.rand.org/pubs/research_reports/RRA869-1.html.

17. "The future is Quantum," Quantum Flagship, last accessed February 7, 2024, https://qt.eu/.

18. *Critical & Emerging Technologies List Update: A Report by the Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council*, The White House, February 28, 2022, https://www.whitehouse.gov/ostp/news-updates/2022/02/28/nstc-critical-emerging-technologies-list-update/.

19. Gordon Corera, "MI5 head warns of 'epic scale' of Chinese espionage," *BBC News*, October 17, 2023, https://www.bbc.com/news/uk-67142161.

20. "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," National Institute of Standards and Technology, U.S. Department of Commerce, July 5, 2022, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

21. The FTC Office of Technology, "An Inquiry into Cloud Computing Business Practices: The Federal Trade Commission is seeking public comments," U.S. Federal Trade Commission, March 22, 2023, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/inquiry-cloud-computing-business-practices-federal-trade-commission-seeking-public-comments.

22. Competition and Markets Authority, "Press release: CMA outlines scope of market investigation into cloud services," Gov.UK, October 17, 2023, https://www.gov.uk/government/news/cma-outlines-scope-of-market-investigation-into-cloud-services.

Authors

Juljan Krause is a Postdoctoral Fellow in Technology and International Security at the UC Institute on Global Conflict and Cooperation (IGCC) based in Washington, D.C. Juljan's expertise is in the international security implications of emerging technologies with a particular focus on the strategic competition between the U.S. and China over quantum technologies. Juljan holds a Ph.D. in computer science and international relations from the University of Southampton in the UK, and certificates in quantum computing and quantum algorithms from MIT. For his doctoral research, Juljan modeled ERGMs on patent data to find estimates of Chinese progress in building up quantum capabilities.

Prior to moving to D.C., Juljan enjoyed a career in the UK civil service where he advised British regulators on quantum tech, AI, and the regulation of digital markets. Juljan received an MSc in the philosophy of science from the London School of Economics and a first degree in economics and mathematics from the University of Frankfurt in his native Germany. Juljan's passion for quantum computing emerged from seminars in the philosophy of maths and physics, and he is always happy to chat about the relationship between science and technology.

About IGCC

The UC Institute on Global Conflict and Cooperation (IGCC) is a network of researchers from across the University of California and the Los Alamos and Lawrence Livermore national labs who produce and use research to help build a more peaceful, prosperous world. We conduct rigorous social science research on international security, the environment, geoeconomics, nuclear security, and the future of democracy; help to educate and train the next generation of peacemakers; and strive to ensure that what we are discovering contributes to a safer world.

IGCC

9500 Gilman Drive #0518, La Jolla, CA 92093-0518