BRIEFING PAPER

409

April 2025

Geostrategic thinking and quantum technology

How promises of quantum technology breakthroughs shape Sino-US rivalry

Markus Holmgren

FINNISH
INSTITUTE OF
INTERNATIONAL
AFFAIRS

FINNISH
INSTITUTE OF
INTERNATIONAL
AFFAIRS

BRIEFING PAPER 409 / April 2025

Geostrategic thinking and quantum technology

How promises of quantum technology breakthroughs shape Sino-US rivalry

Summary

- Disruptive technologies have emerged as key arenas of strategic competition between the United States and China, and, alongside artificial intelligence, quantum technologies are key among them. By influencing current strategies and policies, their implications begin even before innovations materialize.

- Uncertainty about the future and the promised benefits of these technologies have implications for both nations' build-up efforts, resilience strategies, and potential for pre-emptive actions.

- China has made rapid technological advancements in many fields, narrowing the gap with the United States. Examples include the release of an AI application by the Chinese company DeepSeek and China's lead in quantum communication technologies.

- Beyond civilian applications, quantum technology promises significant breakthroughs in military applications, such as codebreaking, signal-free submarine navigation, and intrusion-proof communications.

Author

Markus Holmgren
Research Fellow
Global Security and Governance
FIIA

Introduction

The quantum industry is experiencing a boom. Although useful market-ready solutions are yet to be developed, expectations of revolutionary new capabilities – from codebreaking to secure communications and scientific development – fuel increased investment, research, and development in the quantum industry. These promises of future capabilities also influence geostrategic thinking and actions today, by guiding both build-up efforts and pre-emptive actions to slow down the development of strategic adversaries.

The influence of quantum technologies development is clearly visible in the tech rivalry between China and the United States, driven by growing concerns that one side may gain a major strategic advantage. Figure 1 illustrates this dynamic, as well as the fact that China and the US are far from the only relevant actors in the field, even if they compete with the widest range of strategies and methods. Public funding for quantum initiatives, as shown in the figure, is on the rise, and although its fulfilment is uncertain, it still influences the actions of others.

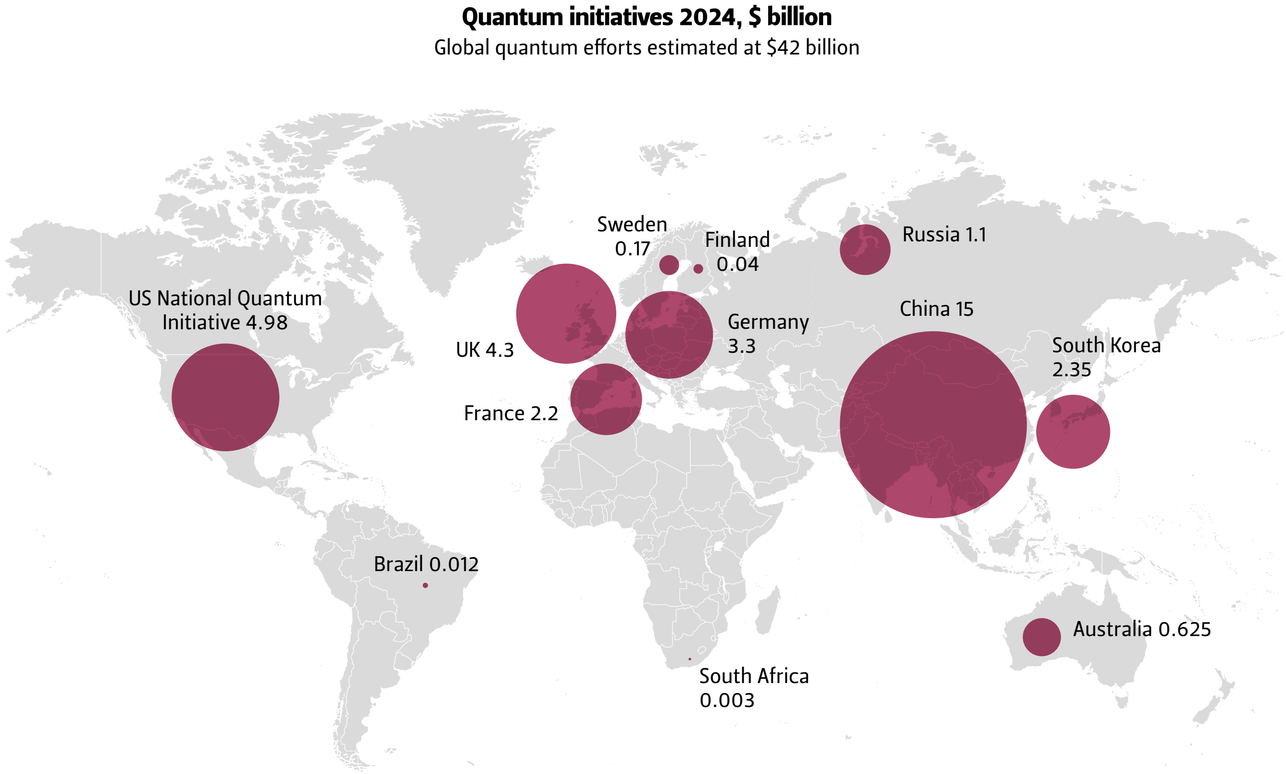

Figure 1. Public funding for global quantum initiatives 2024.
Source: Qureca, https://www.qureca.com/quantum-initiatives-worldwide/

The intensifying tech rivalry increasingly forces companies and research organisations to choose between Chinese or US products in their supply chains. At the same time, global competition for talent has intensified, as many Chinese researchers and engineers who once filled Western research labs have either returned to China voluntarily or been rejected by the US, thus providing China with an influx of returning talent.

> **"While major quantum technological breakthroughs seem certain in the coming decades, the exact timing and manner of such developments are impossible to predict."**

When following the rivalry, it is important to remember that companies often have an interest in giving optimistic assessments of development timeframes to keep investors committed. This creates an illusion of major breakthroughs just around the corner, when in reality, gradual – if increasingly fast – development is much more likely. Many of the systems and devices discussed in this Briefing Paper may still be years and decades away, but their promise is enough to spur geostrategic action today.

This Briefing Paper sheds light on the Sino-US tech rivalry in quantum-enabled fields. It begins with a brief introduction to how promises of future capabilities shape geostrategic thinking and action today. The latter half of the paper then presents key quantum technology-related promises and examples of actions they have spurred.

Geostrategic implications of technological promises

Uncertainty about the future impacts today's geostrategic thinking and action. Uncertainty refers to the gap between known and needed information.[1] Although the future is always uncertain, some events can be anticipated even if their timing and details are unclear. Such events can be called junctures, as they are viewed as pivotal points that shift strategic thinking before and after they occur. Promised events and inventions presented in this paper are such junctures (see Figure 2), and many current policies, such as US restrictions on the export of quantum computing goods to China, are aimed directly at them.

Importantly, these promises relate to tangible products whose 1) location, 2) timing, and 3) manner of development are all uncertain. The key to geostrategic thinking is to devise actions that increase the likelihood of these products being 1) located in one's own or an allied country, 2) developed before anywhere else, and 3) designed in a way that makes copying them as difficult as possible.

While major quantum technological breakthroughs seem certain in the coming decades, the exact timing and manner of such developments are impossible to predict. This makes specific preparations unfeasible and generic preparedness necessary. Global pandemics offer a useful, if limited, analogy. It is statistically certain that humanity will face global pandemics in the future, but predicting the exact year or which virus or bacteria will cause them is impossible. The Covid-19 pandemic came, after all, as a major surprise. Similarly, quantum breakthroughs are certain, but when and how they will happen is unknown.

The key difference between preparing for pandemics and preparing for the ramifications of technological change – quantum or otherwise – is threefold: technological development results from deliberate action, whereas infectious diseases may emerge spontaneously; technological development always benefits someone, whereas infectious diseases rarely do; and while pandemics can often be withstood, technological change is permanent.

This means that it may be strategically feasible to take action in advance to reduce the likelihood that a potential disruptor will achieve a breakthrough before one's own efforts. If a breakthrough occurs despite all efforts, the same measures can be used to slow down implementation and reduce the time that the innovator has a monopoly over their innovation. In the case of intensifying Sino-US quantum technology rivalry, this could involve actions like export controls and other negative sanctions and technology transfer agreements, which the US favours, as well as the talent luring and industrial espionage favoured by China.

---

[1] Galbraith, J. R. (1973) Designing complex organizations. Reading/ Addison Wesley.

Technology	Promise
Quantum computer	Vastly improved natural sciences research capability; able to solve certain tasks, especially those related to probabilities.
Quantum compass (Earth's rotation measurement)	Signal-free submarine navigation.
Shor's algorithm	Revolutionary capability to break encryptions based on factorisation of large integers.
Quantum camera	Enhanced electromagnetic spectrum analysis; usable on smaller platforms with smaller batteries, while reducing congestion on the most common wavelengths.
Magnetic sensor	Mapping various rare earths or man-made structures underground and underwater will enable not only the identification of bunkers, but also analysis of their material composition and the detection of lurking submarines.
Quantum key distribution (QKD)	Establishing uneavesdroppable cryptographic connections.

Figure 2. Examples of technological promises that serve as junctures in geostrategic planning.
Source: Author's own compilation

Technological development always benefits someone, so potential shifts in relative power must be considered in strategic planning. This is crucial for ally-building, as strategic gains by friendly nations are less threatening than those by adversarial ones. For quantum technologies, this highlights the viability of friendshoring – relocating supply chains to politically or strategically aligned countries – and creating path dependencies by investing in platform systems, such as cloud services, office software, and design architecture. While strong path dependencies on quantum solutions are still rare, this is unlikely to remain the case, as first movers set standards for latecomers and serve as platforms for applications. Although the US is cutting back on friendshoring and technology cooperation, its efforts to prohibit European companies from allowing Chinese operators into their supply chains still illustrate this objective.

Technological developments are likely to produce more or less permanent changes, which means that weathering the disruption and bouncing back to the old ways is not an option. Instead, deliberate efforts to adapt to the changed reality are necessary. While old systems can often still be run, the cost of maintaining them increases over time, eventually requiring subsidies to support large parts of the supply chain. Meanwhile, those who have already adapted enjoy the efficiency gains. This highlights the importance of adaptive preparedness, increasing R&D funding and securing critical supplies to limit disruption – all actions that play a significant role in Sino-US technology rivalry.

Following the analysis above, three general types of actions to prepare for unpredictability can be identified. They include:

1. building up capabilities in the field of expected disruption,
2. building adaptive resilience for quick catch-up, and
3. investing in pre-emptive offensive action.

The presented types of actions are not in order of importance, nor should they be seen as alternatives to one another. In fact, a nation's strategic preparedness often depends on maintaining a coordinated flow of information between various sectors and organisations. This is difficult to achieve, but without it, states risk being caught off guard by foreseeable developments.

Quantum technological promises

The quantum technological promises introduced in this section influence geostrategic thinking and contemporary action. Most importantly, they have major implications for Sino-US rivalry. Quantum technologies utilise the quantum properties of very small particles – namely, they take advantage of the fact that, at quantum level, particles behave very differently from larger ones, a phenomenon often referred to as quantum strangeness. Such strangeness

Qubit	A quantum bit. A physical or logical entity with which quantum computations are performed.
Quantum computer	A device that computes, utilising quantum mechanical phenomena.
Quantum sensing and metrology	Systems and methods that utilise quantum mechanical properties for information gathering.
Quantum communication	Systems and methods that utilise quantum mechanical properties for information transmission.
Quantum state	A mathematical description of quantum effects before observation.
Entanglement	A phenomenon where the quantum properties of (groups of) particles are linked, making it impossible to describe them independently.
Polarisation	A type of entanglement notation.

Figure 3. Glossary of quantum terms.

includes, for example, behaviour that resembles waves, where particles appear past an object without passing through or around it, and 'choose' a state of being only upon observation.

For analytical purposes, it is important to note that various quantum technologies benefit from the same research projects and from the general development of one another, which creates synergies and potential for both escalatory growth and major delays. Importantly, these synergies extend to classical sciences and manufacturing. As the technology matures, cumulative growth in fields such as chemistry, biosciences, logistics and the financial sector is estimated to be many times greater than that of the quantum sector itself.

Quantum computing

Quantum computing refers to a method that utilises the quantum mechanical properties of small particles or waves as they travel through quantum logic gates to perform computations. Unlike classical computers, where the basic calculation units (bits) are either charged (1) or uncharged (0), quantum bits (qubits) exist in a superposition of either state. This means that a qubit is not strictly in a definite state, but rather has a probability of being in either state at the same time. These properties enable quantum computers to perform calculations that exploit this phenomenon, but they are also limited by it. For this reason, while quantum computation is eventually expected to supersede the capabilities of classical computers in specific tasks[2] by several orders of magnitude, it is unlikely to develop into a general-purpose technology similar to classical computers.[3]

One of the key challenges in today's quantum computing is that quantum states are very fragile and cannot be observed directly – they must be inferred from their effects. Interaction with the environment causes the quantum state to collapse, ruining its usefulness for computational purposes. This unreliability is called decoherence. As the number of qubits used in a calculation increases, the problems caused by decoherence accumulate. For this reason, with the current quality of qubits, only about 20 can be effectively used in a computation. Adding more qubits does not scale up the computational capability unless improvements in qubit quality or error correction techniques are introduced.

Some developments have occurred in the US, however: Google's new error-correction chip spreads information across multiple qubits by combining several physical qubits into a single logical qubit. This reduces the damage caused when a qubit collapses, enabling computational growth as quantum computers scale up.[4] Importantly, it proves that large-scale computations can be viable without perfect physical

[2] Chou, Charina; Manyika, James; and Neven, Hartmut. "The Race to Lead the Quantum Future". *Foreign Affairs*, 7 January, 2025.

[3] Hughes, Ciaran; Isaacson, Joshua; Perry, Anastasia; Sun, Ranbel F.; and Turner, Jessica. (2021) *Quantum Computing for the Quantum Curious*. Springer Nature.

[4] Google Quantum AI and Collaborators. (2024) "Quantum error correction below the surface code threshold". *Nature* 638, 920-926. https://www.nature.com/articles/s41586-024-08449-y.

qubits. It also marks technological milestone two of six in Google's self-imposed roadmap towards quantum supremacy. It is not inconceivable that the next leap forward could come from China.

Producing a physical qubit that is both sufficiently isolated from interaction and capable of producing observable effects is, however, so difficult that we do not yet know which qubit production method or error correction technique will ultimately prove scalable. For this reason, the quantum race remains genuinely open, with roughly 20 different viable methods and dozens of competing developers.[5] This stands in stark contrast to the AI industry, for example, where the benefits of scaling and the accumulation of early-mover advantages limit market access.

The supply of raw resources critical to quantum computing remains diversified across most qubit production methods, but China's strong position in the field still lends some weight to potential trade sanctions. At the same time, much of the quantum computing design work is carried out in-house using US-based software, which reduces the effectiveness of negative sanctions, except in the services industry. Irrespective of how the situation develops, many producers of critical downstream systems, such as coolants, superconductive materials, cleanrooms, and silicon wafers, are already benefitting from increasing demand.

Quantum cryptography

The key benchmark for the adequate scaling of a true quantum computer is its ability to break all commonly used encryption methods using quantum cryptography. This event, known as Q-day, is the central focal point in quantum computing predictions. Most estimates place Q-day 15 to 30 years in the future, although unexpected developments may also occur.

Quantum cryptography refers to techniques that combine quantum computing with cryptographic methods, most notably encryption and decryption.[6] Put simply, one of the advantages of quantum computers is their ability to explore multiple paths simultaneously. While binary computations always lead to a definite answer and estimations are thus made by chaining together large numbers of smaller-scale computations with definitive results, quantum properties allow computations based on probabilities.

For this reason, commonly used cryptographic methods based on the factorisation of large arbitrary numbers (such as RSA) will become insufficient once the scaling problem is solved. Algorithms to achieve this already exist, with Shor's algorithm being the most well known. However, decoherence currently prevents these calculations from being executed.[7] The first to achieve adequate scaling will gain a temporary unilateral capability to break all non-quantum- proofed encryptions. If that were to happen tomorrow, the access gained would compromise most state, military, financial, and private digital systems. While this outcome is not inevitable, preventing it will require decisive action.

"Importantly, the slower the global quantum-proofing efforts advance, the greater the potential gains from Q-day, making the technology race even more aggressive."

While there are no technological barriers to quantum-proofing all digital systems, the related costs are likely to mean that some systems will remain unproofed when the breakthrough occurs. Which systems – and how many – will have ongoing implications for the intensity of the rivalry.

It is clear that the great powers view the potential ability to break encryptions of protected systems as an unacceptable capability boost for the other side. This suggests that major advances in quantum computing will likely lead to increased funding, secrecy, resilience measures, and pre-emptive hostile action. Importantly, the slower the global quantum-proofing efforts advance, the greater the potential gains from Q-day, making the technology race even more aggressive. The promise of breaking encryption has

---

[5] Dargan, James. "Quantum Computing Companies: A Full 2024 List". *The Quantum Insider*, 29 December, 2023.

[6] See Vidick, Thomas and Wehner, Stephanie. (2023) *Introduction to Quantum Cryptography*. Cambridge: Cambridge University Press.

[7] Monz, Thomas; Nigg, Daniel; Martinez, Estaban A.; Brandl, Matthias F.; Schindler, Philipp; Rines, Richard; Wang, Shannon X.; Chuang, Isaac L.; and Blatt, Rainer. (2016) "Realization of a scalable Shor algorithm". *Science* 6277 (351): 1068-1070.

already motivated a series of so-called 'store now, decrypt later' cyberattacks, with the US National Security Agency (NSA) storing all encrypted data until it can be decrypted.[8] China is undoubtedly doing the same, further motivating the global push to accelerate the quantum proofing efforts.

Quantum sensing and metrology

Quantum sensing and metrology involve the development of new sensors and techniques to measure quantum-level effects. Quantum sensing allows for the measurement of phenomena such as gravity, magnetism, and seismic data with accuracy increased by several orders of magnitude compared to classical sensors. In addition, by using particles for probing instead of chemical or electrical signals, quantum sensors can record a broader range of the electromagnetic spectrum. This enables more detailed multispectral analysis in smaller carriers, reducing energy consumption, and potentially alleviating congestion in the most commonly used wavelengths and orbital slots, which are an increasingly active arena of great power rivalry.[9]

Importantly, unlike quantum computers, quantum sensors already provide tangible benefits. For example, the accuracy of atomic clocks is key to maintaining synchronisation of sensitive communication systems.[10] As the technology matures, its promise for China lies in using it to increase the independence of its financial transmission system, CHIPS, from the US-controlled SWIFT system, which currently facilitates almost all international financial transactions.

Additionally, techniques such as quantum lithography and noise-cancelling development benefit quantum computing, while quantum computers themselves are also useful for quantum sensing. The virtuous cycle was well reflected in the recognition that accurately simulating quantum physics requires a computer based on quantum physics, a major factor that helped launch the quantum computing industry in 1981.[11] The synergy between these fields results in a self-enforcing loop that reinforces the boom, but does not make it inevitable.

Many quantum sensing applications promise direct capability enhancements, especially for the defence sector. For example, a quantum compass could enable highly accurate analysis of the Earth's rotation, allowing signal-free navigation of military submarines – if the scaling up of early prototypes succeeds. This is particularly promising for the US, as its defence posture pivots from Europe to East Asia. In addition, advanced magnetic detection will improve accuracy in mapping various rare earths or man-made structures both underground and underwater. This technology could lead to the discovery of underground bunkers and their material composition, as well as the detection of submarines operating in the depths. This is particularly promising for China, as its nuclear submarine fleet remains relatively small.

Quantum communication

Quantum transmissions utilise polarised photons, where a horizontal or 45° photon denotes 0 and a vertical or 135° photon denotes 1, instead of using short and long wavelengths. This method allows for the creation of a secure communication network, as any eavesdropping would collapse the polarised state of the observed photons, disrupting the transmission in a manner that cannot be hidden or masked.[12]

Using such a quantum communication system for cryptographic key distribution (QKD) can enable secure, currently uncopiable and intrusion-proof transmission over both optic fibre and open air. This will remain the case even after Q-day, assuming quantum-proofing is also implemented. The benefits are clear for both military and state governance. Increased command, control and communications security could eventually lead to a

---

[8] Greenberg, Andy. "Leaked NSA Doc Says It Can Collect and Keep Your Encrypted Data As Long As It Takes To Crack It". *Forbes*, 20 June, 2013. https://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-ca.

[9] Holmgren, Markus (2023) "The role of space technologies in power politics: Mitigating strategic dependencies through space resilience". *FIIA Briefing Paper* 365. Finnish Institute of International Affairs.

[10] Degen, Christian; Reinhardt, Friedemann; and Cappellaro, Paola. (2017) "Quantum Sensing". *Rev. Mod. Phys* 89 (3): 035002.

[11] Clegg, Brian. (2021) *Quantum Computing: The transformative technology of the Qubit Revolution*. Icon Books.

[12] Boileau, Jean Christian; Gottesman, Daniel; Laflamme, Raymond; Poulin, David; and Spekkens, Rober W. (2003) "Robust polarization-based quantum key distribution over a collective-noise channel". *Physical review letters* 92 (1): 017901. See also Ugwuishiwu, Chikodili; Orji, Ugochukwu E.; Ugwu, Celestine; and Asogwa, Caroline. (2021) "An overview of Quantum Cryptography and Shor's Algorithm". *International Journal of Advanced Trends in Computer Science and Engineering* 9 (5): 7487–7495.

paradigm shift in today's information-centric warfare and limit the advantage the US currently holds through its cyber dominance, thus challenging its current military doctrine.[13]

While quantum communication systems like QKD could provide benefits for military and state security globally, China has been particularly focused on these technologies to ensure the secrecy and security of its own communication systems. This partly explains the huge funding push that China has dedicated to quantum communication. For example, in 2017, China successfully dropped packets of polarised photons from its quantum science satellite called Mozi at an altitude of 1,200 km, which carried a key that enabled a secure fibre-optic connection with Austrian partners. The success was the result of reliable long-term funding, and seems to have led to further investment in developing a constellation of quantum satellites, as well as in building the world's first quantum communication backbone. Additionally, the general funding of quantum research in China has rapidly increased.[14]

However, China's subsidy system creates competition whereby the largest subsidies – often funded by regional loans – are granted to projects with the most hyperbolic quantitative indicators. If this is the case, then China faces the risk of bogus projects gobbling up funding from useful projects. This has already been observed in the Chinese AI industry, where corruption and unviable projects have wasted billions of US dollars.[15]

That said, Chinese activity in the quantum field, coupled with aggressive anti-corruption campaigns, staggering patenting activity (see Figure 3), and exaggerated marketing by subsidy-seeking companies is likely to push the US to take further action. However, most Chinese quantum communication patents are only listed in China and might not hold

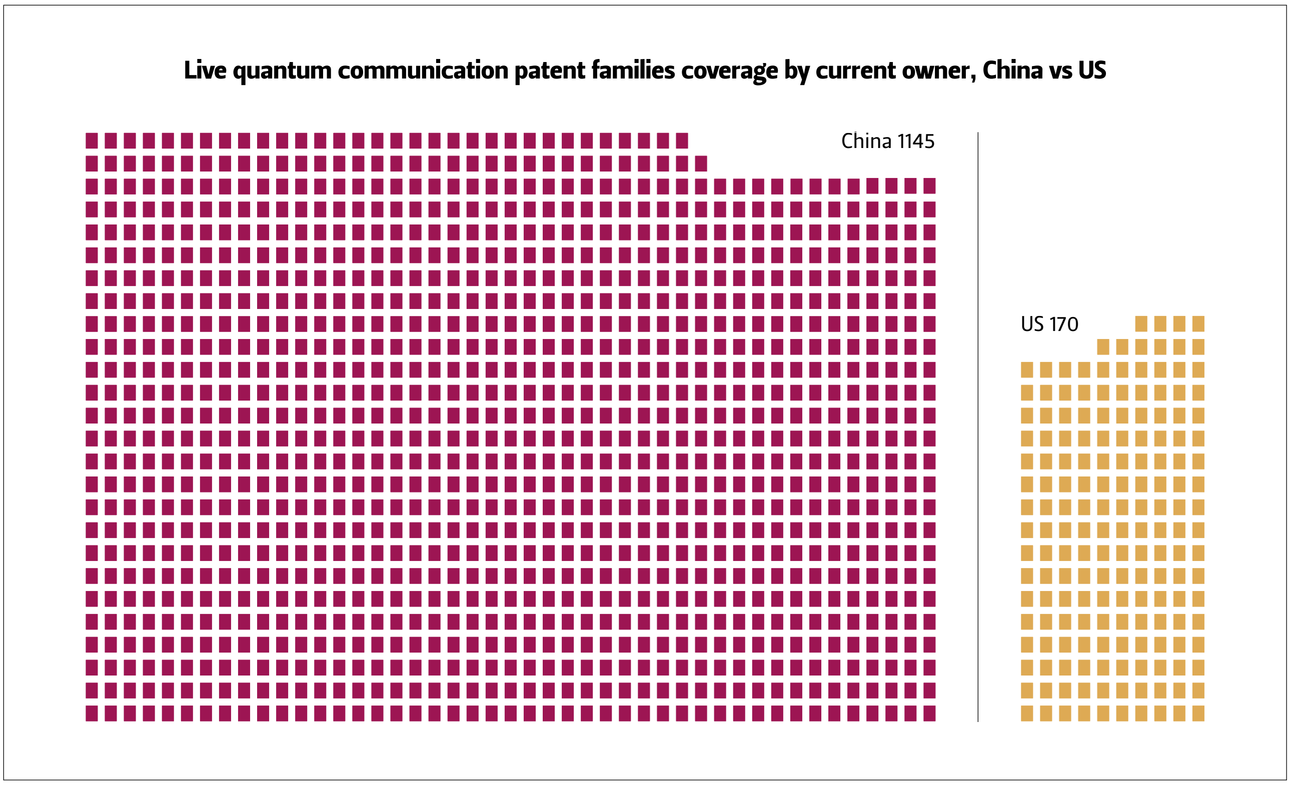

Figure 4. Coverage of live quantum communication patent families by current owner.
Source: Author's own compilation using PatSeer patent registry software

---

[13] Kania, Elsa B. and Costello, John K. (2018) "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership". Center for a New American Security.

[14] Ibid.

[15] Yang, Zeyi. "Corruption is sending shock waves through China's chipmaking industry". *MIT Technology Review*, 5 August, 2022. https://www.technologyreview.com/2022/08/05/1056975/corruption-chinas-chipmaking-industry/.

up in foreign courts. This could be either good or bad for Beijing: good if it allows for the unilateral legitimisation of intellectual property theft, and bad if it leads to reliance on bogus patents that waste time or lead to misguided investments. This kind of statistical misrepresentation could also backfire on China by prompting other countries to increase their own R&D funding and seek tech transfers from China.

Conclusions

Quantum technologies promise to provide answers to problems previously thought unsolvable. These promises have triggered a largely publicly funded boom and have led to a range of geostrategic practices aimed at securing control over the anticipated capabilities. This includes not only the many systems discussed in this paper, but also the benefits for further scientific progress in fields such as chemistry and pharmaceuticals, among many others.

As with any technology, quantum-enabled solutions can be used for good – such as developing new medicines, or for bad – such as developing chemical or biological weapons. The implications of this realisation will not only become tangible when these systems begin operating in the future but have already emerged. The development environment and the ambitions of funders set the tone for future use and can even determine how the fruits of technological advancement are shared.

When following the Sino-US technology rivalry, it is important to pay attention not only to technological advancements in the field, but also to the policies that arise from the promises those advancements make. It is also worth keeping in mind that technology races share the same escalatory tendencies as arms races and trade wars. Threat perceptions and domestic interests typically work hand in hand to enforce this effect. For example, the US defence sector increasingly relies on the threat image of China's technological development to secure additional funding. Presumably, the situation in China is not entirely different, although it is difficult to verify due to the culture of secrecy and unreliable documentation. ⬢

BRIEFING
PAPER
409
April 2025

ISBN 978-951-769-826-9
ISSN 1795-8059
Language editing: Lynn Nikkanen
Graphic design: Joonas Juutilainen
Cover photo: iStock

This Briefing Paper is part of the research project 'China's disruptive technologies and international security', funded by the National Defence Scientific Advisory Board (MATINE).

FINNISH
INSTITUTE OF
INTERNATIONAL
AFFAIRS

Arkadiankatu 23 b
POB 425 / 00101 Helsinki
Telephone +358 (0)9 432 7799
www.fiia.fi

The Finnish Institute of International Affairs is an independent research institute that produces high-level research to support political decisionmaking and public debate both nationally and internationally.

All manuscripts are reviewed by at least two other experts in the field to ensure the high quality of the publications. In addition, publications undergo professional language checking and editing. The responsibility for the views expressed ultimately rests with the authors.