Quantum computing promises new technological possibilities. How close are they?

The U.S. and China are racing to develop computers based on the properties of quantum physics—with implications for science and security.

Donald Keough, *Christian Science Monitor*, June 27, 2026 (shortened)

After fundamentally changing science more than a century ago, modern physics may be about to revolutionize the world of computers—with implications for everything from the speed of doing complex research to nations' vulnerability to cyberattack.

Billions of dollars are pouring into quantum computing—a budding field that relies on the sometimes surprising behavior of subatomic particles to process information. This past week in Boston, Quantum.Tech World was held, with over 1,000 top executives and researchers from more than 40 countries gathering to transition the ideas from the lab to the commercial market.

The White House has recognized the potential for quantum computing. President Donald Trump this week signed executive orders pushing for the creation of a quantum computer for scientific research, use of quantum science by the military, and protections for government computers against quantum cyberattacks by U.S. rivals.

If a technological breakthrough comes, wide-ranging implications will likely follow. Quantum computing poses potential benefits for the academic and business worlds, but also raises cybersecurity concerns, as it could be used to crack security codes that protect computers from hacking.

It might still take years for current quantum computers to reach an adequate level of development. However, higher capital investment and assistance from artificial intelligence have accelerated progress.

"Quantum technology is a really exciting area. It has the potential for major advances," says Steven Olmschenk, an associate professor at Denison University in Granville, Ohio, who researches atomic physics and quantum information. "The path that it takes [to get there] is not completely clear, or how long those things will take … but I think we are definitely on the path to realizing that future."

Dozens of companies, including IBM, Google Quantum AI, IonQ, and Quantinuum, have already created quantum computers, but so far, there is no clear leader in development.

While significant strides have been made, these computers have yet to sufficiently demonstrate full quantum advantage—the ability to deliver savings in resources or achieve higher accuracy compared with classical computing methods.

Although quantum computing is unlikely to ever fully replace current technology, its implications are varied.

Quantum computing could be significantly useful in areas such as chemistry and materials science. According to global technology and consulting company IBM, quantum computing is especially helpful in modeling physical systems and discovering patterns and structures in data that might otherwise be missed. That could be useful in sectors from biology to finance.

But quantum computing could also pose security risks to modern encryption systems. In 1994, mathematician Peter Shor developed Shor's algorithm, a method that could be used by quantum computers to crack RSA encryption, which secures much of today's online communication. While classical computers would take millions of years to crack a frequently used RSA encryption, quantum computers could do so in just days.

To counter this, the United States has spearheaded a Post-Quantum Cryptography Initiative, which led to the development of new encryption algorithms expected to be released as standards for civilian and defense networks by 2027.

As with AI and other technology, China and the U.S. are rivals in the development race. China has recently focused more investment in quantum computing, and designed the world's first dual-core atomic quantum computer.