Newsweek

TECH & SCIENCE

ARE WE READY FOR A 'QUANTUM SURPRISE' FROM CHINA?

BY **FRED GUTERL** ON 10/25/19 AT 1:22 PM EDT

TECH & SCIENCE QUANTUM COMPUTING CHINA

Google engineers built a quantum computer that can perform a calculation in 200 seconds that would take a conventional computer 10,000 years, a feat that can only be described as impressive. But they got some blowback for their claim to have reached a crucial milestone—the point at which quantum computers can outperform conventional ones.

In 2012, John Preskill in *Quanta* magazine dubbed this milestone "quantum supremacy." The Googlers borrowed his phrase in the title of their paper—"Quantum supremacy using a programmable superconducting processor"—in the normally staid journal Nature.

Some engineers from rival IBM Corp. took issue with this characterization. In a blog post, they argued that the *Nature* paper did not describe an experiment that has relevance to any real-world application—and therefore that the quantum-supremacy milestone remains elusive.

Let's hope the IBMers are right. The potential of quantum computers to leverage the weirdness of subatomic physics to perform incredible feats of computation would pose a threat to our data-heavy internet-dependent world.

Most experts don't expect the quantum computing to be ready for prime time for 10 years or more. But that's just a guess. True quantum supremacy would render the most common form of encryption obsolete. Nobody really knows when the moment of reckoning will come when quantum computers will be capable of cracking any code to reveal the secrets of nations, or who will accomplish it first. The implications are fueling a race of sorts, as nations vie for a quantum edge.

The nightmare scenario, from the standpoint of U.S. national security, is that China develops a working quantum computer without tipping its hand. That would leave China free to decrypt secure communications and gain access to reams of U.S. intelligence data. "China could develop quantum computing in secret, earlier than anticipated, and employ it against sensitive communications to out maneuver or strategically outflank the U.S.," wrote Elsa Kania and John Costello in a report for the Center for a New American Security. "The arrival of such a quantum surprise would be difficult to assess and judge, and could confound U.S. intelligence assessments."

It's hard to overstate the potential for disruption that quantum computing represents. Current methods of encryption, developed in the 1970s, rely on mathematical complexity to deter hackers. Data is scrambled and can be unlocked with big numbers called "keys," which only senders and receivers possess. Without the key, cracking the code would take a calculation so large that it would take an eternity even with the world's best computers.

A quantum computer, however, would make current encryption measures obsolete. Rather than manipulating bits, quantum computers take advantage of a peculiar quality of subatomic particles to exist in more than one "state" at a time. The physicist Edwin Schrodinger famously likened this "superposition of states" to a cat being both dead and alive at the same time. A particle of light (called a photon) can be made to represent 0, 1 and other values all at once. A quantum computer can manipulate these particles to perform many calculations simultaneously, vastly increasing the speed at which it can solve complex problems, such as cracking encryption.

China has made quantum computing a strategic imperative. Although China has been accused of stealing technology in the past, its quantum computing effort is home-grown and substantial. It reportedly spent $400 million on new research labs in Anhui province. China is not the only country developing quantum technology--the U.S., Europe and Japan also have projects in the works. An $80 million NSA project to build a quantum computer, called Penetrating Hard Targets, was revealed among the documents leaked by Edward Snowden.

To protect against quantum hacking, nations are developing a form of quantum encryption that would harden communications against quantum hacking. Rather than using numerical keys to encrypt data, a quantum communications network would employ particles such as photons. In a 2017 experiment, China's Micius satellite beamed photons to two different ground stations 1200 kilometers apart. The photons at one ground station were "entangled" with the photons at the other ground station. Entanglement is another oddity of quantum physics whereby two particles are somehow linked—Einstein called it "spooky action at a distance." Entangled particles could serve as unhackable keys to encrypted transmissions.

Micius is the first of a planned constellation of satellites that would serve as the backbone of a Chinese quantum communications network. China has also built a 2000-kilometer quantum trunk line between Beijing and Shanghai and has plans to extend the network nationwide.

To forestall a quantum surprise, standards organizations are already planning for new encryption protocols that would leave data less vulnerable to quantum computers. Moving to a new encryption scheme that didn't rely on large numeric keys would require a vast retooling of data communications.

U.S. policymakers also worry that China accomplish in quantum computing what it did in 5G communications: catch the U.S. industry flat-footed. What's needed, they say, is some kind of industrial policy in Washington. "We have really strong tech companies," says Christopher Painter, former top diplomat on cybersecurity at the U.S. State Department. "But if we really want to maintain an edge, we need to take this seriously at a strategic level."